ISO/IEC JTC 1/SC 27 N 2248rev1

REPLACES: N 2248

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	Summary of National Body Comments
TITLE:	Revised summary of NB comments on ISO/IEC WD 15446 (SC 27 N 2172), Information technology - Security techniques – Guide on the production of Protection Profiles and Security Targets
SOURCE:	National Bodies of Canada, France, Germany, Japan, United States
DATE:	1999-04-14
PROJECT:	1.27.22
STATUS:	This document replaces SC 27 N 2248, and is being submitted for consideration at the 18th SC 27/WG 3 meeting in Madrid, Spain, April 19 – 23, 1999.
ACTION:	**ACT**
DUE DATE:	1999-04-19
DISTRIBUTION:	P, O and L-Members L. Rajchel, Secretariat JTC 1 K. Brannon, ITTF W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners M. Donaldson, Project Editor
MEDIUM:	Server
NO. OF PAGES:	56

Secretariat ISO/IEC JTC 1/SC 27, DIN Deutsches Institut für Normung e.V., 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: passia@ni.din.de

ATTACHMENT 1
to SC 27 N 2248rev1

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2172 P -member voting: Canada

Title: Comments on N 2172, Guide for Production of PPs and STs, Version 0.6

Date: March 12, 1999

Source: Canada

Canada has the following comments.

Major Technical:

#	P	C	Pa	S	Comment
M1		ALL			This document is adequate for producing a Protection Profile (PP), but requires further work to be useful as guidance for those producing a Security Target (ST). The problem is that STs are written from a much different point of view than PPs. While PPs are written as a statement of ”I Want”, STs are written from a point of view of ”I Will Provide”. Most of the detail within this document is written from the point of view that the author of the PP/ST is the owner of a security problem, and is working on how to best address this problem, and this is the point of view of a PP writer. An ST writer, however, is likely to be producing a specification to address a particular security environment or in response to a Request For Proposal (RFP), where the RFP will list requirements for the system, but may not present information in a format that can be readily pulled directly into an ST. Guidance is needed to help explain to the ST author how they can address RFPs and user requirements, and how they can refine PPs and properly reference them in an ST.
M2		6.5, 7.4.2, 8.4.2, etc.			The TOE composability issue needs to be addressed in a more comprehensive method with pointers for how PP/ST writer would address a large system architecture. For example, if a TOE system was composed of 50 different IT components, how many PP/STs should be written? Should there be: 1) 50 individual STs written plus the overall TOE ST; 2) One ST for the TOE system; or 3) Between 1 and 50 STs depending on where the ST writer wants to divide the system?

M3					Two new sections titled ”PP/ST Introduction” and ”TOE Description” should be added before section 3, and two new sections titled ”PP Claims” and ”PP Application Notes” should be added after section 8, to correspond with the PP and ST structure.
M4					A new section ”PP Claims” is needed, to explain how to properly reference an existing PP that addresses only one part of the TOE. This will provide information on how to refine the PP security components, and also how to combine it with new functionality and all other information, in order to develop the ST.
M5	50	A			The checklist is not complete with respect to the PP and ST content. The checklist should also address PP/ST Introduction and TOE Description.
M6		A.6			By comparison A.5 contains significantly more information on PP rationale than A.6 on ST Rationale. Section A.6 should be expanded to include information on all 4 types of rational, namely Security objectives rationale, Security requirements rationale, TOE summary specification rationale, and PP claims rationale.
M7		D			The worked example in Appendix D needs to be modified to include information on the PP/ST introduction and TOE Description, and PP Claims.
M8		D – F			Instead of having multiple appendices, each of which provides some detail on what a PP/ST would look like for a particular type of TOE, it would be preferable to have a single worked example that is more thorough and rigorous in its level of detail. In particular, the TOE Summary Specification section could benefit from a greater level of detail, since this is an area which is not covered by PPs. Perhaps there could be two separate Appendices which address the same type of TOE. The first appendix provides a PP for the TOE, and the second appendix provides an ST which corresponds to the PP in the previous Appendix, and provides detailed guidance on completing operations for the functional requirements, completing the TOE Summary Specification, and filling in the PP claims section. There are many PPs already created by the Common Criteria Project and other government organizations so these appendices should be greater emphasis should be on developing the ST writing capability and hence the details for how to complete those sections unique to the ST should be especially rigorous.

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2172 P -member voting: Canada

Minor Technical:

#	P	C	Pa	S	Comment
T1		ALL			This document should be separated into two different parts, one for PP guidance and one for ST guidance. That division would ensure a clear approach to writing the respective sections by ensuring that all points were addressed and written according to the needs of the respective writer.
T2		8			Currently a ST writer must read the PP and ST Rational sections 7 and 8 to figure out how to develop a ST Rationale since the PP rationale is a subset of the ST rationale. Reading both sections is difficult since the ST writer has to interpret the meaning of PP rationale in terms of ST rationale and sort out the non-essential pieces and duplication. A separate and concise section exclusively for the ST writer would be more helpful.
T3	19	3			This document should be modified to provide guidance to the ST and PP writers to indicate that a TOE security policy (TSP) is necessary, and is partially specified through the use of components from CC Part 2 families such as FDP_IFC or FDP_ACC. This additional guidance will address the TSP requirement which has been weakened by the statement in the CC Part 3, Version 2.0, May 1998, CCIB-98-028, Page 96, Para 2 Application Note, line 3 which states ”The developer is not explicitly required to provide a TSP, as the TSP is expressed by the TOE security functional requirements, through a combination of security functional policies (SFPs) and the other individual requirement elements”.
T4	10	3.3	1		This paragraph states that the ”statement of threats may be omitted if the security objectives are derived solely from the organization security policies”. Since a user requirements or RFP typically state the ”security problem”, we suggest a new sentence added as follows ”The statement of threats may be omitted if the security objectives are specified via the security policies stated in an RFP”.

ISO/IEC WD 15446
Reference number: ISO/IEC JTC 1/SC 27 N 2172 P -member voting: Canada

T5		5			This document should state that it is advisable for the IT security requirements to be copied into a PP/ST, in order that all the text is in one place. These CC components need to be replicated in the ST even if there are no selection, assignments, or refinements made to a particular component since the TOE must still be evaluated to the functional and assurance components. Furthermore, by listing the components in the ST in this manner, it facilitates the ST writer and Evaluator consistency check of the TOE functionality and prevents errors by flipping between the ST and the CC constantly.
T6	21	5.1	9		Item (a) starting with "*assignment*" should indicate that the assignment operation may, in some cases, allow a NULL value t be assigned.
T7		C			A section should be added that explains the relationship between the CC cryptographic functional components (in the FCS class) and the FIPS 140-1 requirements. This is necessary since it is claimed that an ST can be developed to represent a product, which can also be submitted for a FIPS 140-1 validation. The market place requires this information as there have been RFPs recently issued in the United States requiring a TOE that is compliant to both the CC and FIPS 140-1 standards.

French comments related to the Working Draft 15446 "Guide for production of PPs and STs"

Chapters 1 to 9:

Section 3.5.2, 1st para: It is not clear why it is required that PP/ST for composite TOE should specify the security environment for the composite TOE in full. The CC allows ST to make PP claim, and to specify additional information where applicable.

Moreover, it is not required for composite ST/PP to restate all the security objectives (see section 4.4.2). So why should it be required for the security environment statement.

Section 3.5.2, 3rd para: It is the composite TOE PP/ST which has to be consistent with component PP/ST, and not the opposite.

Section 5.1: The paragraph dealing with operations is not consistent with the CC. CC allows to perform iteration and refinement operations to both types of requirements, functional and assurance ones. Do not limit these operations to functional requirements.

Section 5.2.1: The figure provided does support the relationship between principal and supporting SFRs. Modify the figure or remove it.

Section 5.2.1 is mostly dedicated to the identification of supporting SFR. This is quite surprising because the CC does not support this delineation between two categories of SFR. Moreover, it seems that supporting SFR is defined as an SFR required to satisfy dependencies.

Section 5.2.1: The two last paragraphs contradict each other.

Section 5.2.2: The paragraph ” Where assignment or selection ... be presented as ” has to be modified to make clear that all completed satisfied operations have to be identified (assignment, selection, but also refinement and iteration).

Section 5.4.3: The CC allows also explicitly stated assurance requirements to be defined, and not only functional requirements.

The third sentence of the paragraph is false. Explicitly stated components may be reused.

Section 8.3.8, 2nd para: The TSS shall not be presented as providing additional details in comparison with security requirements. It is an interpretation to reuse the result of the analysis of mutual support at the level of security requirements for the analysis of mutual support at the level of the TSS.

Annex B:

Section B.1: The example threats do not implement the advice given in Chapter 3 section 3.3.3 (it is proposed to label threats with " TE ".

Section B.4: Same comment than previously concerning the example objectives.

Annex C:

It is not clear why a specific annex is dedicated to cryptographic functionality. It seems that cryptography-related assets are considered separately from other types of assets to be protected. There is not rationale for this, and the CC does not support this delineation.

Section C.3.1.3: The forms of attack listed in this section apply to all types of IT assets, and not only cryptography-related ones.

Tables 10 and 11: Most of threats and objectives listed in these tables are a restatement of the ones listed in sections B.1 and B.4.

Section C.4.5.7: Electromagnetic emanations are out of the scope of the CC. Related information should be removed from the guide.

Section C.5: There is no relationship between this section and the goal of the document. Remove this section.

N°	Chapter	Page	Remarks
1	Global		There are too many pages in this document. Some things are repeated many times. For example, for the definition of threats, there is : - pages 10 to 13 : definition of what is a threat - page 50 : advices in how to write a threat - pages 54 to 55 : examples of threats This is too much.
2	Global		There should be interesting to do references to the part 1 and part 3 of the CC in this document. These references would permit to know exactily what requirements are covered.
3	1.2	1	Last sentence of the first paragraph : if the TOE is a specific IT system, there is no interest to do a PP. It should be more interesting in this case to do directly a ST. → remove this sentence.
4	4.1	16	item b) : how can someone say the description of an objectif is "concise" ?
5	4.2	17	It is difficult to define one objectif for each of the major groupings of security functionnal requirements that will be specified in the PP or ST because when the author of the PP is writting the security objectives, he has not already chosen the requirements which will be included in the PP ! So, he can't know the major groupings of security functionnal requirements that will be specified in the PP or ST.

6	4.3	18	It's indicated that an appropriate starting point to specify the security objectives for the environment is to identify "one security objective for each threat, policy or assumption". Why ? There is no reason to specify "one" objective for "one" threat, policy or assumption !
7	figure 3	20	There seems to miss two lines in the figure : - from CC Part 2 to Security Functionnal Requirements - from CC Part 3 to Security Assurance Requirements
8	5.1	21	refinement : the refinement allows the PP or ST author not only to restrict the possible solutions to a given SFR. The refinement can be useful to explain in what conditions the requirement is used, to indicate who are the users, … This remark is also applicable page 24 and 25.
9	5.2.1	22	In the CC, there is no distinction between the principal SFRs and the supporting SFRs. Why introduce this distinction ?
10	5.2.1	22	There is no figure 4 in the document. → Change the reference.
11	figure	23	This figure has no number. Thus, this figure is the same as the figure 3 page 20.
12	5.2.1	23	first b) : if these additional SFRs are necessary to ensure that the security objectives are achieved, there should be in the "principal SFRs".
13	5.2.4	26	It would be interesting to give more details for the class FMT. In the part 2 of CC, when there are management activities, it's difficult to know in what requirement of the FMT class these management activities have to be include.
14	5.2.6	27	FMT_MSA.3.1 example : in this example, a part of the requirement which is not an operation has been changed. I think a PP author has no right to modify the text of the requirements. He only can complete operations. If he wants to give details or to adapt a part of the requirement, he can add a refinement.
15	5.5.2	31	If a TOE is composed with components which have different assurance requirements, how is calculated the assurance level of the complete TOE ?
16	figure 5	32	In this document, the SOF claims appears only in ST. In the CC, this is although a requirement for a PP (APE_REQ.1.10C in part 3 (page 34) and page 40 in part 1).
17	6.5.1	34	Why is this paragraph in "Composability issues" ? It should be an independant paragraph.
18	figure 6	36	An arrow between "IT security requirements" and "TOE objectives" is missing.
19	7.3.4	38	a) : why is it necessary to include multiple rows if there are multiple occurrences of a component ? In all occurrences, the dependencies are the same !

20	7.3.4	38	b) : I don't understand the goal of this item.
21	7.3.4	38	c) : I don't understand what is to be done in this item.
22	7.3.4	38	e) : if the components are labeled as in the CC, there is nothing to do (it's immediate) !
23	7.3.4	39	first paragraph : in the CC, there is no obligation to include all auditable events of the components if FAU_GEN.1 is retained ("the following actions should be auditable …"). So the PP author hasn't to provide reasons if he has judged an auditable action is not necessary.
24	7.3.4	39	What is described here for mutual support is not what is required in France by SCSSI !
25	7.3.4	39	FPT_RVM.1 : this component is in the part 2 of the CC, but it should be in the part 3 as it doesn't provide functionnal requirement but assurance requirement. So, il should not be mentionned in this guide.
26	7.4.2	41	a) : if the security objectives of the composite TOE are not exactly the same as those in the individual components, it should be interesting to map each security objective onto the security objectives of the individual components to demonstrate that all security objectives in the individuals components are covered by the composite TOE.
27	7.4.2	41	b) : in the composite TOE, there can be more functionnal requirements than in the individual components. In this case, the ST author has to explain why he has chosen these requirements.
28	7.4.2	41	c) : the dependencies on the IT environment have to be satisfied or justified in each of the individual component. So, I don't understand this item.
29	7.4.2	41	d) : last sentence : how can this be done ("the composite TOE PP rationale must address interrelationships or dependencies between different components") ?
30	8.1	42	first sentence after the figure : this is a ST-specific aspect. This should be in the figure 7.
31	8.3.6	44	c) : not only. The ST author has although to show that there is no conflict between the additional requirements.
32	8.3.9	45	What is described in this paragraph is not realist. For example, how can it be demonstrated that the assurance component ADV_RCR.1 is addressed by an assurance measure ? There will be no assurance measure for this component !
33	8.4.1	45	This paragraph doesn't address composability issues.
34	8.4.2	45	id remarks 26 and 29.
35	9.2.2	46	last sentence : "should" is not the good word. "must" should be better. Why specify a functional package if it doesn't define any security objectives ? If the package contains functional requirements but doesn't explain why these components are needed, there is no interest. It seems although necessary to include in the package a rationale which shows the security objectives are covered by the functional requirements.
36	Annex A	50	This annex is not really necessary as there are examples in the guide.

37	A.4.2	53	This is different from the paragraph 8.3.9. In paragraph 8.3.9, all assurance requirements have to be addressed by an assurance measure and not only those requiring specialist methods or techniques.
38	B.6.1	59	Not all the functional requirements from the part 2 of the CC are presented in this table. Why ? (example : FAU_SEL.1)
39	Annex C	63	Why is this annex in the document ? There is no reason.
40	Annex D, E, F	91	There is today a lot of PPs that have been evaluated in the world. There is no interest to put in this document an example which has been completely created for the guide.
41	D.1.1	91	last sentence : if these aspects are only in the security objectives for the environment, these objectives will be traced back to nothing and it will not satisfy the assurance requirement APE_OBJ.1.3C during the evaluation.

ATTACHMENT 3
to SC 27 N 2248rev1

Japanese Comments on ISO/IEC JTC1/SC27 N2172

Title: Guide on the production of Protection Profiles and Security Targets
Source: JAPAN
Date: March 30----------Comment 1:Clause 3.3.3 How should threats addressed by the TOE environment be handled?
This section is not appropriate position because that threats addressed by the TOE environment must be identified after decision of security objectives in ” 4. The Security Objectives”. Threats are not identified but security objectives are identified from the viewpoint of countermeasures by TOE environment.

Comment 2: Clause 5.1 Introduction b) , page 22
Assurance level seems to be specified not by SFRs but by operational environment of TOE.
Change b) as follows;
b) Security Assurance Requirements on the TOE . These identify the required level of assurance in the operational environment of TOE.

Comment 3: Clause 5.2.3 How should the audit requirements be specified?
There should be clear criteria for specifying either a minimum, basic, or detailed level of auditing.

Comment 4: Clause 7.3.3 How to show the strength of function claims are appropriate?
There should be clear criteria for specifying strength of function claims.

Comment 5: We propose ”A table of threats and security objectives” as an annex.
There should be a reference this annex from ”3.3 How to Identify and Specify the Threats” and ”4.2 How to Specify Security Objectives for the TOE”.
Attachment is ” A table of threats and security objectives ”

US comments on SC27 N2172 ”Guide for Production of PPs and STs”, December, 1998.

1. Introduction

US comments on SC27 N2172, ”Guide for Production of PPs and STs, hereafter referred to as the Guide, are organised as follows:

Section 2. Summary of our overall impressions
Section 3. General comments on the Guide
Section 4. Specific comments on specific paragraphs

2. Summary of Overall Impressions

The overall impression is that this Guide is a viable and useable tool for its intended purpose. However, several revisions may yet be necessary to enhance its usefulness.

This Guide does have some very good points. A new person to the Common Criteria (ISO 15408) might have a difficult time interpreting the difference between a PP and a ST. The Guide does an excellent job in demonstrating this difference. This does not mean that more robust explanations of PPs’ and STs’ purposes are not recommended. See the recommendations in the comments below. Appendix A does a very good job of wrapping up the entire process and it may be the most useful part of the Guide.

Unfortunately, in its current form, the Guide appears to omit much needed guidance and includes information that may be misleading. Some areas of this Guide could be made clearer, as a Guide should attempt to be as unambiguous as possible. The Guide could also suggest ways to write a PP and ST to overcome some of the grey areas in ISO 15408, such as interoperability requirements. As authors of PPs and STs gain more experience, revisions to this document should be made to address the shortfalls and pitfalls found.

3. General Comments

3.1 The Guide has been reviewed with reference to FDIS 15408, the "Common Criteria" version 2.0, with ISO-identified errata applied. References in the Guide should correspond to that ISO nomenclature.

Recommendation: All references in the Guide to "Common Criteria" or "CC" should be changed to "ISO 15408".

3.2 Comments are based on the interpretation that the purpose of this Guide is only for direction and reference, not as a ”rule set” establishing a standard of how to author a PP or ST. Given that it is an ISO/IEC document, a reader may have the tendency to view the document as the rules for PP or ST creation rather than as pure guidance. Guidance documents may have portions that are inconsistent from the regulatory or standards documents from which they are derived.

Recommendation: Explicitly address the scope and purpose of the Guide in greater detail, clarifying that this document is an informational ISO Technical Report and therefore is not intended to provide authoritative interpretations of ISO 15408, nor is it to become a de facto standard for the creation of PPs and STs. Words to the following

effect should be added to the front material to ensure that the Guide is not used in this fashion:

"This Guide is provided for guidance only. This Guide should not be cited for authority on content or structure for the evaluation of PPs. If there is any inconsistency between this Guide and International Standard 15408, the latter takes precedence."

3.3 Annex A of this document contains the essential information needed for producing PPs and STs and is very useful, especially for readers who are familiar with the Common Criteria.

Recommendation: A paragraph should be added in section 1 to inform the readers about the summarised guidance in Annex A, so some of them can take advantage of the well documented checklist. The way Annex A is currently presented (in item j of section 1.4, Document Structure) does not clearly convey its value.

3.4 There are many audiences that this document will be applicable to, each having a different set of needs. Therefore, only specific sections of this Guide might apply a given audience.

Recommendation: Include pointers in the summaries to allow for the various audiences to quickly move to the section of interest. Also, optimise redundancies where possible.

3.5 The concept of packages is described in the Guide. However, there is no reference as to where or how to use them in the chapters giving PP and ST production guidance. The document states that a package is ”intended to be reusable, aiding in the construction of PPs, STs, or larger packages”. If the package’s use is not included in the guidance, packages may never be used or reused.

Recommendation: The use of packages should be incorporated and discussed in detail in what is currently Chapter 9 of the Guide, and there should be reverse references to this guidance in the functional and assurance requirement sections of chapter 5.

3.6 The only example not included in the appendices is an example of a package.

Recommendation: To make packages viable entities, an example should be included. However, the example should include a reminder stating that the example is not intended as a standard, as ISO 15408 does not specify requirements on functional or assurance packages.

3.7 ISO 15408's information about the purpose of a PP could usefully be expanded upon to permit clearer understanding. Section 1.2 of the Guide discusses PP and ST content and use, but its statement of PP purpose could likewise be improved.

Recommendation: A specific explanation of purpose is proposed below.

3.8 It is conjectured that some PP readers are potential TOE consumers and are thus casual readers who may not get past the first two or three sections of a PP. Yet the Guide does not include any guidance on development of the PP Introduction and TOE Description. Although it is true that the Guide is oriented towards PP developers and not users, inclusion of guidance on these sections will benefit the latter.

Recommendation: Specific suggestions for new sections on the PP Introduction and TOE description are given below in Sections 4.3 and 4.4.

3.9 The Guide does not contain a Glossary

Recommendation. Add a Glossary. Terms common to both this Guide and to ISO 15408 should contain the exact same definitions (i.e., use in the Guide Glossary those

definitions that appear in clause 2.3 of ISO 15408-1). Add to it definitions of any technical terms introduced in this Guide which were not included in ISO 15408. In addition, include terms whose meanings are not well known and those that have multiple common meanings.

3.10 The Guide should clearly explain the proper use of all optional portions of a PP or ST. For example, the Guide needs to discuss the use of requirements for the non-IT environment. Recommendations on addressing the non-IT environment are scattered through Section 4 of these comments, marked by the keyword ”non-IT”. Other optional sections include the use of non-ISO 15408 Assurance requirements and the use of Application Notes. The latter are discussed briefly in Section 4.9 below.

3.11 Most the comments presented here either recommend additional material or attempt to strengthen the intent of existing material. However, there are some specific places where the content of the Guide is questioned. In particular, the treatment of composability throughout the Guide is not presently acceptable. There are also a few places where stylistic differences are noted.

Recommendation. See detailed discussion and recommendations on composability below. Please carefully consider the other comments and either change the existing advice or, at a minimum, acknowledge legitimate differences of view.

3.12 The principal references (CC2, CC2A, and CC3) are quite large. Note also that CC2A no longer exists in the FDIS version of ISO 15408.

Recommendation. Citations will be much more useful if readers are told where to look within a particular volume. Include specific section and page numbers where possible. Remove all references to Part 2 Annex as a separate volume.

3.13 The draft Guide was has been presented online in a single document format (Adobe PDF).

Recommendation. Publication of the Guide in multiple formats including HTML will facilitate broader use of the document. Specifically, an HTML version will facilitate its use in online help facilities for ISO 15408-based tools currently under development.

3.14 The examples appear to exclusively use TCSEC C2 and B1 type security functionality.

Recommendation. Either broaden the scope of the examples or include a disclaimer explaining why the scope of the examples was limited to C2/B1 security functionality.

3.15 The purpose of Annexes C and D has not been made clear. They are highly redundant with the main chapters and seem to add little additional information.

Recommendation. Specifically state the purpose of these Annexes so the reader of the Guide can determine if these Annexes are of any use to them.

3.16 Theoretical Approach - The guidance presented follows a very logical top-down approach while the pragmatic bottom-up approach is often necessary in real examples.

Recommendation. It would be good to have some examples of more realistic threat analysis: for example, a developer selects passwords for I&A. Once this mechanism is selected, then the developer analyses the threats against it: password cracking, network sniffing. Given these threats, the developer may then need to go back and modify the mechanism.

3.17 Composability is not a trivial problem. ISO 15408-1 is silent on composite or component TOEs. There is currently little understanding of how systems of products will be handled under ISO 15408.

Recommendation. Please remove all discussion and guidance on composability currently contained throughout the Guide and instead insert at the beginning of the document, perhaps in the Scope section, a brief statement to the effect that composability is a complex problem and is currently still under study. State that when clear guidance is available it will be provided as either an addendum to this Guide of as part of a future version of the Guide. In particular, the material in 5.5 and 5.5.2 suggests that the environment be allowed to satisfy TOE requirements. This should not be allowed.

3.18 In identifying the security environment, very little is mentioned about required interoperability with other IT devices in the environment. There often are specific critical operational requirements for the TOE to inter-operate with a trusted IT device that, in turn, must satisfy certain security functional or assurance requirements for the users' assets being protected. These specific interoperability requirements need to be evaluated to ensure the trusted IT device can perform its security functional and assurance requirements. However, the scope of the TOE evaluation does not need to include the security functional or assurance requirements that must be satisfied by the other IT device. This is briefly discussed in paragraph 1.3 (Functional requirements paradigm) of ISO 15408-2, "TOE interfaces may be localised to the particular TOE, or they may allow interaction with other IT products over external communication channels". As examples, an intrusion-detection system might automatically update an access control list on a router or protection policy on a firewall, or Security Application Software might interact with the OS it resides on. This interoperability will be critical in offering real-time security protection.

This area is tied in with composability and dependencies. There are many suggestions that can be made to resolve these inadequacies. However, due to the complex nature of composability, interoperability and dependency, any recommendation here should be used as part of the collaborative work needed to make the appropriate resolution.

Recommendation. As a potential suggestion in the future for this Guide, discussions could be placed in the dependency subparagraphs throughout the Guide addressing required interoperability issues. These discussions might include the following guidance on organisational policy and security objectives:

"In some cases the TOE may have critical operational requirements to inter-operate properly with a trusted IT device that provides security functional or assurance requirements. However, in the scope of the TOE evaluation, it is not necessary to evaluate the security functional or assurance requirements provided by the trusted IT device. If the security policy mandates that the TOE inter-operate with other devices in the environment, statements should be included to ensure that evaluators can adequately examine the TOE's capability to inter-operate as mandated."

For example, such a policy might read, "The edge ingress/egress device will provide initial access control, and other security devices will automatically update access control at this edge device, in as much as it practical to do so."

A corresponding security objective, in this case, might read, "The TOE must automatically update access control as prescribed in the security policy P_INTEROP".

3.19 There seems to be confusion between the terms environment and IT environment throughout the Guide. This is compounded by ISO 15408's use of these terms.

Recommendation. In order to clear up the confusion between the terms, Section 4.3 should explain that objectives for the environment might address both IT and non-IT objectives, and should offer examples of both (Section 4.3 currently reads as if it focuses on non-IT environmental objectives only). It should be pointed out that security requirements are the only place that ISO 15408 expects the delineation between IT and non-IT to be made, along with it being optional. Care should be taken, in all other sections of the Guide that mention environment to carefully delineate between IT and non-IT when appropriate.

3.20 One problem especially relevant to writing STs is the level of detail required. Should a ST contain an overview of how a product meets a requirement, or should the ST simply assert that it meets the requirement? For example, for security functional testing, should the ST contain a summary of how the vendor performs functional testing, or should the ST simply state that the vendor does perform the required tests (period).

Recommendation. The Guide should expound about the level of detailed required.

3.21 The guidance needs to better accommodate system development over the life cycle, especially for large systems and long life cycles (such as 20 years). Many systems evolve over their life cycle. Evolutionary system development may be practised. The PP for such systems will also evolve. Any of the components of the PP may change. Constraints such as mission, funding, environment, and schedule may change. Parts of the system may be built under different constraints.

Recommendation. PP guidance for such conditions is needed.

3.22 PPs may be employed as part of a contract between a sponsor/purchaser and a developer or system integrator. Information not relevant to the contract will be more profitably packaged separately. Contractual language may be preferred to ISO 15408 terminology.

Recommendation. Guidance should be provided for such usage.

4. Specific Comments

Specific comments on the Guide are organised with respect to the document's paragraph and subparagraph numbers: The paragraph number in parenthesis is the section of the reviewed document.

4.1 - Section 1, Introduction

4.1.1 (1.1) This section contains too many commas.

Recommendation. Delete extra commas. In the third paragraph, either delete the comma or else replace "and" with "or with."

4.1.2 (1.1) The statement that reads "It is assumed that the readers are familiar with Part 1 of the Common Criteria" is somewhat contradictory to the primary audience, and also uses incorrect ISO terminology. The primary audience is authors of PPs and STs. To do a complete job of writing these documents they should also be familiar with ISO 15408-2 and 3. There are many discussions in ISO 15408-2 and 3 that explain, in

greater detail, the thought and scope of what goes into PPs and STs. (e.g., ISO 15408-2 paragraph 1.3, Functional requirements paradigm)

Recommendation. Assume familiarity with all three parts of ISO 15408; capitalise on the guidance given in ISO 15408-2 and 3.

4.1.3 (1.1) Objective and Intended Audience: When consumers/users are developing and administering IT security and are using PPs and STs as background information, it is important to understand what guidance the PP or ST authors used during the document's authoring. The consumer/users are critical about the structure and source of any evaluation's information. The guidance on how a PP or ST is built is therefore extremely critical for the users to trust and have confidence in.

Recommendation. It may be wise to add a short statement about the consumer/user community as a secondary audience. This document should be addressed to the consumer/user as well. If it is not, a separate document should be generated as a user specific guide.

4.1.4 (1.2) This subsection is a mix of PP/ST content and use; it does not successfully explain purpose.

Recommendation. The discussion of content can wait until Section 2; replace the present discussion of content with the following explanation of purpose:

"**Purpose of a PP.** The purpose of a PP is to state a security problem rigorously for a given system or product and to specify security requirements to solve that problem. The particular product or system is called the PP's target of evaluation (TOE). A PP thus includes several related kinds of security information:

- "A statement of need identifying, in terms appropriate for users of information technology, the security problem to be addressed.
- "An environmental description refining the statement of need with respect to the intended environment of use, producing the threats to be countered and the policies to be met in light of specific assumptions.
- "Objectives refine the environmental description, giving additional information about how, and to what extent, the security needs are to be met.
- "Security functional requirements and assurance requirements solve the problem posed by the statement of need, as refined by the environmental description and the security objectives. The security functional requirements explain what must be done by a TOE and its environment (including the intended users of the TOE) to meet the objectives. The assurance requirements explain how reliably the TOE security functions must be implemented to meet the objectives.
- "A rationale demonstrates that the functional requirements and assurance requirements suffice to meet the statement of need. The environmental description must explicate the security concerns found in the statement of need. The objectives must explain what is to be done about the security concerns found in the environmental description. The security functional requirements and assurance requirements must meet the objectives.

"[Editorial note to Guide authors: Sometimes the rationale is explained in terms of the pairwise consistency of adjacent PP sections. This is wrong, as pairwise consistency does not ensure overall consistency.]

"For profiles whose statement of need includes threats to be countered, the objectives explain how the threats are to be countered, and how reliably. Threats may be countered in several ways. Some threats may be thwarted by IT security functions; some may simply be detected and recovered from through any available means. In any case, the purpose of a countermeasure is to reduce vulnerabilities and to support security policies of the PP sponsor. Residual vulnerabilities may remain after the imposition of countermeasures.

"A PP's security functional requirements are expected to separate responsibility for security protection into what the TOE does and what the environment does. However, the PP's security functional requirements should not dictate how these functions will be implemented. For this reason, a PP is said to provide an implementation-independent security description.

"**Purpose of an ST.** An ST is like a PP, except that it contains additional implementation-specific information telling how the PP's requirements are realised in a particular product or system. Thus, the ST contains the following additional information not found in a PP:

- "A TOE summary specification that presents TOE-specific security functions and assurance measures.
- "An optional PP claims portion that explains which PPs the ST extends, and what additions or refinements have been made, if any.
- "Finally, the Rationale contains additional evidence establishing that the TOE summary specification ensures satisfaction of the implementation-independent requirements, and that any claims about PP conformance are satisfied."

4.1.5 (1.2, para 3 and 4, page 1) Item (b) duplicates the first sentence or two of the following paragraph. The second phrasing is clearer.

Recommendation. Replace b) with the following recasting of the paragraph that follows item b):

"b) A PP or ST may be used as a means of communication among the party responsible for managing the development of a system, the stakeholders in that system and the entity responsible for implementing that system - hereafter referred to as the developer. In this environment, the ST is proposed in response to the PP. The content of the PP and ST may be negotiated among the players."

4.1.6 (1.2, para 4, pages 1, 2) There seems to be some ambiguity about which kinds of TOEs this paragraph refers to.

Recommendation. Preface the remaining portion of this paragraph (the part not duplicated by item (b) that begins "The content of the PP and ST ...") with the clarifying phrase "In the case of a system PP, ".

4.1.7 (1.3) This section is a poorly worded repetition of a fragment of Section 1.5.

Recommendation. Delete Section 1.3.

4.1.8 (1.4) This section accomplishes little that is not already achieved with more elegance by the Table of Contents.

Recommendation. Replace Section 1.4 with something along the lines of a traditional Executive Summary. Give explicit guidance for readers who are prone to read only

sections they are interested in. In particular, say early on that some readers may wish to begin with Appendix A to get a better feel for the content of the Guide.

4.2 - Section 2, Overview of a PP and ST

4.2.1 (2.2, first para) The first sentence incorrectly states that ISO 15408-1 Figure B.1 (as expressed in the Guide's Table 1) defines the "required" structure of a PP, while the correct characterisation is that the stated contents are mandatory but the structure is recommended. Further, it does not explain whether this figure specifies minimal content, maximal content, or both. This error in the Guide may lead to writing unsuccessful profiles, as several optional PP sections (and some not so optional sections) are omitted from Table 1 despite being necessary in many PPs. Key examples include at least the following:

1. PP1.? Related PPs (cf. Section 2.5, para 2 of the Guide).
2. PP1.? Organisation of the PP (essential for readers not familiar with the typical or actual PP structure; cf. Section 4.3 of our comments).
3. PP1.? Referenced documents (crucial for large-system PPs and for PPs that depend on previously defined IT environmental components; see a previous comment for an example where the Guide acknowledges this).
4. PP3.?? Separate environment subsections for various components (domains) in the TOE IT environment (cf. Previous comment, Case A, on Section 5.5.1 of the Guide).
5. PP5.?.? Requirements that may be satisfied either by the TOE or by the environment (cf. Previous comment, Cases B and C, on Section 5.5.1 of the Guide).
6. PP5.? The need for non-IT requirements (described in 15408-1, clause B.2.6(b) as "often useful in practice".
7. PP7.? Optional rationale for the Introduction and TOE Description.
8. PP7.?.? Separate Rationale subsections for Necessity and Sufficiency of Objectives .
9. PP7.?.? Separate subsections for the following Requirements Rationale topics:
   - Necessity of Requirements
   - Sufficiency of Requirements
   - Dependencies
   - Strength-of-Function Requirements
   - Deferred Operations
   - Extended / Explicitly-Stated Requirements
10. PP?? Glossary of terms (crucial for PPs whose primary audience uses terms in ways that conflict with those of ISO 15408).
11. Alternatives for the rationale to be packaged as a separate document and for the application notes to be inserted in the relevant sections. See the last sentence in ISO 15408-1, clause B.2.8.

A related, perhaps less serious discrepancy between the Guide's Table 1 and good PP authoring is that some optional sections are pictured without identification of the fact

that they may be optional (thereby encouraging specification bloat via the inclusion of irrelevant material. Specific examples include the following:

1. 3.2 Threats (when objectives are derived only from Organisational Security Policies and assumptions).
2. 3.3 Organisational Security Policies (when objectives are derived only from threats and assumptions).
3. 5.3 Security Requirements for the IT Environment (when none are required).
4. 6 Application Notes.

Recommendations:
1) Change first para of 2.2 to read: "ISO 15408-1 annex B, Figure B.1 defines the required contents of a PP. Although the PP structure given in that figure is not mandatory, it is strongly recommended. Table 1 below translates this into an example contents list. Note, however, that there are a number of optional sections or more detailed sub-sections that should also be considered for inclusion. These are identified in context below."
2) Insert the contents of the list above as amplification of the paragaraphs following the table.

4.2.2 (Table 1, 2.2, Table 2, 2.3) The prose in the 4th paragraph of 2.2 and the 5th paragraph of 2.3, ”This description covers the assets requiring protection, the identified threats to those assets...” leads a reader to think that assets should be enumerated separately from threats, organisational security policies (OSPs), and assumptions. The description of the assets should be contained in the threat section, as described in paragraphs B.2.4(b) and C.2.4(b) of ISO 15408-1.

Recommendation. Perhaps a better way to express this sentence could be ”This description covers the identified threats to the assets requiring protection (along with a description of those assets), any organisational...”. Additionally, order the sentence in accordance with the table, i.e., assumptions - threats - policies.

4.2.3 (2.2, Table 1, row 5 and following discussion)

Recommendation. Point out that PPs where the environment has several distinct components may profitably depart from this structure by including separate subsections for the various components of the IT environment.

4.2.4 (2.3, First sentence and Table 2) Earlier comment applies here as well.

4.2.5 (2.3) The Security Target Contents are described with the exception of ”Protection Profile Claims”.

Recommendation. For consistency, a paragraph should be included to give an overview of the PP Claims, as had been done with the other ST paragraphs.

4.2.6 (2.?) Section 2 may be the best place to talk about audience analysis, that is, about the multiple intended audiences for a PP/ST.

Recommendation. Here is some information that needs to be provided:

"One of the key challenges in writing a PP or ST is to factor the presentation so that all of the PP’s intended audiences are properly served:

- "Consumers (possibly including high-level decision-makers) need a general understanding of what conforming TOEs will provide in the way of security. For successful PPs, this may be the largest class of readers.

- "Developers (including implementers in the case of an ST) need unambiguous requirements on how to build conforming TOEs.
- "TOE users (including installers, administrators, and maintainers) need information on the required TOE environment.
- "PP/ST evaluators need information that will justify the technical soundness and effectiveness of the PP or ST.
- "TOE evaluators need information that will justify the claimed compliance of TOEs with associated STs and PPs."

PPs and STs are designed in such a way that different sections serve different audiences, and they need to be written accordingly.

The TOE Introduction, TOE description, and Environment sections should be written for consumers. The Objectives section may be also written for consumers. Alternatively, the PP objectives may be summarised in preceding sections - the PP introduction should clarify which approach is taken.

The TOE Requirements section of the PP should be written for TOE developers. Similarly, the TOE Summary Specification section of a ST should be written for TOE implementers. If these sections are not self contained, they should explicitly indicate which other PP sections (e.g., the PP Glossary) and which other documents (e.g., referenced encryption standards) are necessary for a full and accurate understanding of the presented requirements. In particular, if the TOE Summary Specification depends for its meaning on the TOE Requirements section, this fact should be explicitly pointed out.

Ordinarily, PPs do not directly dictate what is told to TOE users about particular TOEs but do provide essential information that must be passed along to them in an appropriate form. Assurance class ADO requires that such information be passed along. Usage information may occur in several places in a PP, including the Assumptions section, the Environmental Objectives section, and sections on Requirements for the Environment.

Evaluators must be familiar with all sections of a PP or ST. However, information intended primarily for evaluators should be presented in the PP's Rationale section.

4.2.7 (2.4, first para, last sentence) The assertion that the requirements section of an ST should be identical with those of a referenced PP not only encourages excessive size in PPs but contradicts excellent advice given in Section 5.4.1 of the Guide.

Recommendation. Recast this sentence to be consistent with Section 5.4.1.

4.2.8 (2.6) There may be dependencies on the non-IT environment as well as the IT environment.

Recommendation. Extend this discussion of composability issues to include dependencies on the non-IT environment.

4.2.9 Proposed Section on the PP/ST Introduction

As noted in the general comments, this section of a PP is a most important part of the Guide, since the PP introduction is its most-read portion.

Recommendation. In work with PP's, the following guidance has been found to be helpful:

PP Identification

This section should contain the following kinds of information:

- PP name, authors, PP evaluation status, ISO 15408 Version, EAL level,
- Caveats on Evaluation Results, key words, Catalogue Information, etc.

The ISO 15408 Version needs to be included for reasons of version control, although ISO 15408 does not explicitly call for it.

ISO 15408 does not dictate where the EAL level is included, but it is recommended that the EAL be placed here, as it plays a prominent role in international mutual recognition.

The Caveats on Evaluation Results should also be placed in the introduction for the same reasons. As enumerated in ISO 15408-11, clause 5.4, these are:

a) Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are only based upon functional components in Part 2.
b) Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2.
c) Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are in the form of an EAL or assurance package that is based only upon assurance components in Part 3.
d) Part 3 augmented - A PP or TOE is Part 3 augmented if the assurance requirements are in the form of an EAL or assurance package, plus other assurance components in Part 3.
e) Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements are in the form of an EAL associated with additional assurance requirements not in Part 3 or an assurance package that includes (or is entirely made up from) assurance requirements not in Part 3. Caution is recommend in the writing of Part 3 Extended PPs and STs. Mutual recognition does not currently support this kind of PP, as there is no agreed upon basis for evaluating extended assurance requirements.
f) In the case of an ST, there is an additional caveat: Conformant to PP - A TOE is conformant to a PP only if it is compliant with all parts of the PP.

Catalogue data should meet the requirements of WD 15292, Protection Profile registration procedures.

PP Overview

According to ISO 15408, the Overview should be a summary of the PP in narrative form, usable as a stand-alone abstract for use in PP catalogues and registers. A top-level overview of the security problem being solved with the PP should be included but is not explicitly required. A top-level overview of how the PP contributes to the solution is also advisable.

In the likely case that the intended consumer audience for the PP includes high-level decision-makers, the PP Overview should be expanded to an Executive Summary.

Related PPs and Referenced Documents (Optional)

[The material already in Section 2.5, paragraph 2 of the Guide, pertaining to related PPs can go here.]

A PP for a large distributed system will naturally incorporate several other documents by reference (previous threat studies, high-level summary documents bearing on the

TOE description, and documents describing various components of the TOE environment. Such documents may have been developed over a span of years and written by multiple organisations. Such documents may well represent inconsistencies with regard to terminology, viewpoint, environment, and objectives. In such cases, it is important for the PP to carefully explain what is and is not being taken from documents that are being incorporated by reference. The PP's Rationale should address any intentionally unresolved inconsistencies between the PP and relevant external documents.

PP Organisation (Optional)

Readers not familiar with typical PP structure will need an explanation of PP structure and organisation. It the PP's structure must depart significantly from that recommended by ISO 15408-1, then an explanation of structure is needed by all readers. This explanation of structure is traditionally presented in a document's introduction. In the case where ISO 15408-1 recommended structure is used, the following boilerplate may be inserted (optional variants are indicated in bracketed italics): [Editorial note: the following material was compiled directly from ISO 15408-1, Annex B.]

The main sections of the PP are its TOE description, TOE Security Environment, Security Objectives, IT Security Requirements, and Rationale. [If the PP includes non-IT requirements, then the Requirements section is more accurately identified as just "Security Requirements."]

The TOE description provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the PP's evaluation.

The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. [If there are distinct domains for the TOE environment, optionally include the following: The security environmental aspects are discussed separately for distinct domains of the TOE environment.] The TOE security environment includes descriptions of a) assumptions regarding the TOE's intended usage and environment of use, [omit item b) or c) if appropriate:] b) threats relevant to secure TOE operation, and c) organisational security policies with which the TOE must comply.

The security objectives reflect the stated intent of the PP. They pertain to how the TOE will counter identified threats and it will cover identified organisational security policies and assumptions. Each security objective is categorised as being for the TOE or for the environment [include if appropriate: or both].

[The first sentence on Requirements takes various forms, depending on which ISO 15408 Options are selected by the PP/ST author:

- Option 1, TOE Requirements only: All of the requirements in this PP apply to the TOE itself, as opposed to the TOE environment.]
- Option 2, TOE and IT environment only: The IT Security Requirements section provides detailed requirements, in separate subsections, for the TOE and its environment.
- Option 3, TOE and environment, including the non-IT environment: The Security Requirements section provides detailed requirements, in separate subsections, for the TOE and its environment.]

The IT security requirements are subdivided as follows: (a) TOE Security Functional Requirements, [include if AVA_SOF.* is included in the assurance requirements: including strength-of-function requirements for TOE security functions realised by a probabilistic or permutational mechanism,] and (b) TOE security assurance requirements.

[Optional: The Application notes contain additional supporting information on (Explain the PP's use of Application Notes)]

The Rationale presents evidence that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

The Rationale is factored into two main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them.

4.2.10 Proposed Section on the TOE Description

As noted in the general comments, this section is an important part of the Guide because the TOE Description is likely to be of interest even to casual readers.

Recommendation. In work with PP's the following guidance to be helpful:

The TOE Description should contain the following kinds of information:

- Product Type
- General TOE Functionality
- TOE Boundary (optional)
- TOE Operational Environment (optional)
- Key Assumptions about the TOE (Optional)

The general TOE functional description is just that. It is not just a description of TOE security features, unless the TOE is a special-purpose security product. The TOE description may be more useful if it includes a description of the TOE Boundary and Operational Environment.

The TOE Boundary description tells what is in the TOE and what is not. It is possible for the PP to provide some flexibility between environment and TOE in compliant STs. But the range of allowable choices should be bounded and explicit.

The Operational Environment description tells where the TOE is used, covering important assumptions, business process constraints, and other key elements that are of most concern to higher-level PP users.

Finally, this section should include key assumptions about the TOE itself that play a significant role in the PP's Rationale. Corresponding key assumptions about the TOE environment are presented in the Assumption subsection of the PP's Environment section.

4.3 - Section 3, The Security Environment

4.3.1 (3.1 itemised list) Bullet (b) is not explicitly in ISO 15408-1 or 3. The assets requiring protection is the first set of information needs to be identified when identifying

the threats. In addition, the organisation of section 3 indicates that there are three categories of ”security problem” to be addressed by the TOE: assumptions, threats, and organisational security policies.

Recommendation. Suggest that (b) be combined with what is now c to form a new b.

4.3.2 (3.1, para 2, item (b), clarifying example) The primary assets requiring protection by a fielded system are typically outside the TOE, and they are typically not information. However, it is acknowledged that they are also often not knowable to a developer/PP author.

Recommendation. The parenthetical in bullet (b) should also mention assets outside of but protected by the TOE.

4.3.3 (3.2) In ISO 154081, clause B.2.8a implies that the PP objectives rationale must treat assumptions similarly to threats and OSPs. Specifically, their inclusion requires some explicit or implied response by the objectives. In practice, it has been observed that an assumption may be used merely to justify lack of need to consider certain threats and thus, lack of corresponding requirements.

Recommendation. Point out that stating an assumption requires the PP author to know how (and whether) the TOE will respond to it (e.g., attempt to check or help enforce its correctness). Mention that the objectives rationale requires that assumptions, as with threats and OSPs, must be covered explicitly or implicitly by objectives.

4.3.4 (3.2, list on page 10) There are several other kinds of assumptions that ought to be discussed.

Recommendation. Recommend that the following be considered for inclusion in the environmental assumptions portion of the PP:

- Key assumptions of the PP author that influenced the development of the PP.
- General assurance needs (e.g., assumptions that led to the choice of an EAL).

4.3.5 (3.2, para beginning ”In line with the general principle ...,” last sentence) The proposal to represent detailed requirements for the non-IT environment, as ”Objectives” sets up an artificial lack of parallelism between IT requirements and non-IT requirements. ISO 15408 provides no support for this asymmetry. Indeed, it explicitly discusses requirements for the non-IT environment in Part 1, Annex B.2.6 (b), describing them as ”often useful in practice.” Part of the problem here is that the Guide gets a little ahead of itself. This same issues regarding non-IT requirements crops up later in connection with objectives for the environment.

Recommendation. In this section, place more emphasis on non-IT assumptions by giving more examples of non-IT assumptions (e.g., the intended users of the TOE are young children). Change the guidance to acknowledge the existence of requirements for the non-IT environment. See Comments 4.6.12 and 4.7.39 for related changes that are needed in connection with Objectives and Requirements.

4.3.6 (3.3) If a prudent job is not completed in identifying the threats, the security requirements will fall short of adequate protection and may leave the organisation’s assets at an unacceptable risk level. One of the hardest portions of an organisation’s risk analysis is accurately identifying and defining the threat. Even though risk analysis is beyond the scope of ISO 15408, this guidance document should do a better job of advising its audience where resources for threat identification and risk analysis can be found.

Recommendation. Point out the importance of risk analysis. Emphasise that a risk analysis done by a PP/ST author without much experience in threat identification will potentially degrade the viability of the PP or ST. Give references to the literature on risk analysis.

4.3.7 (3.3) This section did not discuss whether the violation of a policy is to be regarded as a threat.

Recommendation. This section should discuss the violation of policy to state ”policy violations should not be treated as threats”.

4.3.8 (3.3, para 2, first line) The word ”is” is used where ”be” is correct.

4.3.9 (3.3.1 b) In defining ”what the assets need protection from,” it is critical that the vulnerabilities that exist in the assets’ environment be identified. The environmental description of a PP or ST does not directly address the vulnerabilities in the environment of the organisation’s assets. (Do not confuse this discussion with the Assurance requirement family, AVA, which discusses the vulnerabilities of the TOE.)

Recommendation. It would be prudent to make a reference to a vulnerability analysis for derivation of what the assets need protection from. Vulnerability Analysis will identify some of the potential vulnerabilities to an organisation’s assets and allow for greater accuracy in defining threats. In projecting a security environment, relevant threats are only those that take advantage of the vulnerabilities present. As a suggestion paragraph 3.3.1 (b) could read, ”What do they need to be protected from in regards to the vulnerabilities in their environment?” Also, the author should be aware that a vulnerability analysis of the environment might not be in the scope of ISO 15408. Therefore, a footnote should be appended to paragraph 3.3.1 b) that caveats this and gives the intended audience suggestions as to resources available that discuss vulnerability assessments. Also, the author must be aware that vulnerability analysis is not an exact reflection of all potential security holes and should not underestimate the possibility of new and undiscovered threats. In defining the threat agents in the security environment, the author of the PP or ST must be extremely careful to address the relevant threats that meet today’s and potentially tomorrow’s vulnerabilities.

4.3.10 (3.3.1 c) In defining the level of technical expertise one may assume that this is quantifiable. Quantifying the level of technical experience is becoming more difficult. With all of the automated tools for hacking and probing networks and the increase in their availability, one’s technical experience is becoming less of a factor when looking at potential damage or compromise to an organisation’s assets.

Recommendation. When identifying threat agents, it is suggested that a footnote be added suggesting the author of the PP or ST consider the availability of automated assets to the threat agent when considering the level of expertise. Also, point out that due to the widespread availability of automated attack tools, expertise may not be as significant as it once was.

4.3.11 (3.3.1, para 2 and footnote 1) There are a number of significant concerns with this important paragraph and the accompanying footnote:

1) (Non-TOE assets) The discussion of assets must be significantly broadened to encompass the real-world situation that the TOE must protect information and/or functions within the TOE that directly and/or indirectly affect other assets that are outside of the TOE. Information within the TOE almost always represents secondary assets whose utility or value can be ascertained only from an examination of its influence on external tangible assets. Those external assets are

typically not even IT assets, though it is true they may not be known at the point of PP construction. In 15408-1, subclause 2.3, the following non-exclusive definition is given: "Assets - Information or resources to be protected by the countermeasures of a TOE." A PP's threats should therefore address all resources (assets) of interest to the PP sponsor that are affected by the system, not just the IT assets within the system. Failing to include non-IT assets in the threat analysis where they are known can lead to seriously flawed PPs in which protection of the TOE itself is superficially achieved while potentially allowing the TOE to be used as a primary instrument of attack against highly valued assets in the TOE environment. Therefore, due consideration, where feasible, must be given to threats to assets both inside and outside of the TOE that may be compromised through misuse of the TOE. While it is acknowledged that PPs may characteristically address general requirements of a user community, rather than specific threats in a known environment, and therefore specific extra-TOE assets in the abstracted environment may not be readily identifiable, due consideration of these assets when they are known is needed to understand the motivation of human threat agents, the impact of successful attacks, and the kinds of IT protection that will be useful in protecting the assets.

2) (Owners) Use of the term "owners" in this paragraph requires clarification. It is legitimate to refer to those who have an interest in protecting those assets from harm (hence diminishing their value) as owners. However, it is important to point out in the Guide the complexity of "ownership" in order to stress to the PP writer that care must be taken as the community of interest may be complex.

3) (C-I-A) Confidentiality, integrity, and availability are being used in the last sentence in a manner inconsistent with some commonly given definitions. See related discussion below regarding 3.3.1, para 4, item (b).

4) (Footnote 1) The footnote is inconsistent with the definition of the term "assets" in ISO15408-1. As noted just above, ISO 15408 generalised that term, and thereby accommodated a broader view of security and of threats in particular. The Guide should be careful to be consistent here and elsewhere with ISO 15408 definitions and not rigidly equate asset with IT information asset, as currently done in this footnote. By contrast, consistency with [GMITS] is less important because the Guide claims to be about ISO 15408, not about [GMITS].

<u>Recommendations:</u>

1) Change the presentation to clearly distinguish between (a) assets that the TOE can directly control (typically but not always informational assets), and (b) assets that can be attacked through misuse of the TOE (normally not just informational assets). Point out that the actions of the TOE are directly implicated in protecting both kinds of assets.

   - The Guide should carefully point out that key assets requiring protection - including informational assets - need not be within the TOE. A typical example would be a PP for the control subsystem for a large distributed system. In this example, the subsystem serves as a central point of attack and may be used to lay waste to all of the controlled subsystems, even if the attack leaves the central control system relatively unharmed. Another even more familiar example is a network firewall. By design, the primary assets to be protected are not within the firewall but behind the firewall.

- The Guide should carefully point out that, in terms of risk analysis, the primary assets requiring protection are often not information. In the case of a bank, the primary assets of a banking system are money, entrusted to the bank by its customers. In the case of a system for controlling aeroplanes, the primary assets requiring protection are the planes, their crew, and their passengers.

2) Point out that in many situations, the primary assets requiring protection will have multiple owners who differ from the owners of the TOE and of the information that the TOE contains. Where appropriate (i.e., where the anticipated usage of the TOE supports it), these primary owners should be identified. Give some simple examples:

   - The US Federal Aviation Agency may own a computer that contains information provided by airlines for the protection of passengers; the primary assets are the passengers who are owned by themselves rather than the FAA or the airlines.
   - In a Domain Name Server (DNS), different domain names have different owners, all of whom may differ from the owner of the DNS.
   - In the case of medical systems, it is commonly held that the TOE's information has no single owner, but rather consists of all those having an interest, due to the extremely complex rules and considerations guiding its use and control.

3) Use confidentiality, integrity, and availability in this paragraph consistent with the resolution of the comment regarding 3.3.1, para 4, item (b).

4) Change the footnote to achieve consistency with ISO 15408 by stating a commitment to use its definition of assets, even if this means being inconsistent with [GMITS].

4.3.12 (3.3.1, para 3) This paragraph forgets that threat agents are not necessarily human, especially in Item c). This directs PP authors to ignore some threat agents at the expense of others.

Recommendation. Rework the entire paragraph. For item c), substitute ”capabilities” for ”expertise” and qualify ”motivation” with ”in the case of a human agent.”

4.3.13 (3.3.1, para 3, items (a) and (b)) There is an unexplained lack of parallelism here - ”abuse” in (a) and ”compromise” in (b). The more common term in the Guide is ”compromise”.

Recommendation. Replace ”abuse” with ”compromise” in Item (a).

4.3.14 (3.3.1, para 4, item (b)) Confidentiality, integrity, and availability are being used in a manner that is inconsistent with some commonly given definitions. For one thing, not all attacks may be understood as being against confidentiality, integrity, and/or availability, even if these three terms are defined quite broadly. As discussed later in the Guide, some attacks are indirect or preferably called security-protection attacks against the TSF itself. For another, many glossaries (including some published by ISO) define confidentiality, integrity, and availability in simplistic terms that do not begin to cover all of the bad things that can be done with information. The undefined use of these terms in this context may be confuse naive readers and directed them to consider certain kinds of attacks while ignoring others.

Recommendation. Introduce a new subsection that discusses the kinds of informational loss that may result from an attack. This is the place to introduce the

distinction between direct and security-protection attacks. This section should also explicitly introduce the broader definitions of confidentiality, integrity, and availability that are necessary in order to make item (b) accurate, even for the limited case of direct attacks. Here are the requisite definitions:

- Availability - the presence of information or resources, when and where they are needed, in a usable form.
- Confidentiality - the protection of information from inappropriate or unauthorised release.
- Integrity - See Data Integrity, Correctness Integrity.
- Data Integrity - the protection of data from inappropriate or unauthorised modification.
- Correctness Integrity - correctness of information, specifically correctness of assertions and instructions. A correct assertion is true. A correct instruction is legitimate in the context of the organisation in which it is issued.

4.3.15 (3.3.1, last para) In virtually every other discussion of risk analysis, authors are careful to point out that one must consider not only the probability (or expected frequency) of attack, but the expected magnitude of tangible loss resulting from a successful attack. Omitting loss as an essential aspect of risk analysis compounds previous errors regarding the nature of assets by covering up the fact that magnitude of loss typically cannot be assessed without consideration of non-IT, tangible assets. This omission encourages PP authors to consider attacks independently of whether the attacks cause meaningful loss, resulting in PPs, which specify TOEs, that protect against things nobody really cares about.

Recommendation. Provide more detail about risk analysis. Include the need to assess loss resulting from successful attack. Point out the role of tangible assets in assessing loss.

4.3.16 (3.3.2 and 3.3.3) It is not clear if sections 3.3.2 and 3.3.3 are intended for specifying threats addressed by the TOE and by the TOE environment respectively.

Recommendation. If so, the title of section 3.3.2 and the last sentence of both sections 3.3.2 and 3.3.3 should be changed to reflect that. There are separate sections for specifying security objectives for the TOE and for the environment (section 4.2 and 4.3 respectively).

4.3.17 (3.3.2, second paragraph, item (a)) This line seems to suggest that threat agents are human and that one should use the more general term ”threat source” when referring to the general case. Unfortunately, this is not how terminology is used in ISO 15408.

Recommendation. Generally speaking, the Guide should not only support ISO 15408 terminology but also discuss its ramifications in such a way as to further the reader’s understanding. Suggest devoting a paragraph to threat sources (a.k.a. threat agents) and the fact that they’re not all human.

4.3.18 (3.3.2, paragraph 2) Item c) ”form of attack” is not equivalent to explanation of ”threat scenario.” Threat scenarios are useful only as examples of general descriptions. Minor variations in scenarios or even introduction of new approaches may still be categorised under the same type of attack.

Perhaps there are PPs that can defend only against specific scenarios, but they are probably a degenerate case. Protection should be afforded to classes of attacks.

Recommendation. Recast the presentation to point out this distinction between ”form of attack” and ”threat scenario.” Item c, in particular, should read:

c) attack scenarios that can accomplish the threat (e.g., ...)

4.3.19 (3.3.2, second paragraph, the examples) Guidance should be more specific on how to describe the assets to be protected. The examples given do not identify the assets that need protecting; they only give the assumption that the threat agent may gain access with which to exploit the asset.

Recommendation. Discuss possibilities for what the asset is (the account, the data accessible from the account, the processes that can be launched from the account, etc. Point out that protection objectives and requirements derived in regard to the environment would be totally different based on identification of assets. For example, protection requirements for an empty warehouse would be different than the same warehouse full of nuclear weapons.

4.3.20 (3.3.2, third paragraph) A major point of potential confusion is the distinction between high-level threats and detailed threats.

Recommendation. Recommend referring to detailed threats as (detailed) attacks to facilitate distinction between the two kinds of threats. In any case, do explain the distinction:

Detailed attacks have associated attack scenarios, whereas high-level threats typically may be carried out through a variety of different attack scenarios. Moreover, a single threat agent typically carries out a detailed attack, whereas multiple threat agents acting in collusion may mount a high-level threat.

Clearly emphasise the distinction between high-level threats and detailed attacks. Point out that the Threat sections of most PPs list high-level threats rather than detailed attacks for sake of brevity and better coverage.

4.3.21 (3.3.2, paragraph 3, first sentence) For the most part, the Guide’s use of terminology is consistent with the distinction given above. A confusing exception occurs in the first sentence on page 17.

Recommendation. Fix this sentence by deleting the phrase ”of the threat scenario.”

4.3.22 (3.3.2, paragraph beginning with ”Overlap between threats ...”, first sentence) This paragraph gives good guidance, but the first sentence overstates the benefits of the guidance.

Recommendation. Restate the guidance as ”Overlap between threats can be more easily avoided if....”

4.3.23 (3.3.2, page 13, paragraph beginning ”The advantage of ...”, second sentence) This paragraph understates the disadvantages of mnemonic labels.

Recommendation. Recast the second sentence as:

”However, there are also several potential disadvantages to the use of labels:

- ”it may not be possible (due to practical constraints limiting the number of characters in the label) to assign a meaningful label in all cases;

- ”in some cases the label may be misleading or ambiguous (as when the label is a commonly used term with a broader or different meaning);
- ”the same label may occur in multiple profiles with different meanings, leading to unintended confusion by those who read both profiles.”

4.3.24 (3.3.2, last paragraph) It isn't agreed that one should avoid including "indirect attacks" on the TOE security functions as part of the threats. The paragraph is not convincing, nor does it provide an adequate explanation where and how such threats should be specified. Furthermore, the Guidance here is contradictory to ISO 15408-1 paragraph C.2.4 (b), which clearly states that all threats that are relevant to the secure operation of the TOE shall be listed. "Indirect attacks", more precisely called "security-protection attacks", are relevant to the secure operation of the TOE. Contrary to what is claimed, it has been found that security-protection attacks can be described without undue assumptions about the nature of the TSF. See: [http://niap.nist.gov/TnC%20HTML%201/Catalogue%20Queries/Loss%20Category%20vs%20Loss%20Category%20.html]. This index contains four sections; the fourth is a list of security-protection attacks of general interest.

Recommendations:

3.2.2, last paragraph, should be changed in the following ways:

- The distinction between direct attacks (a.k.a. primary attacks) and indirect attacks (a.k.a. security-protection attacks) needs to be more clearly stated and more heavily emphasised: Clearly explain the difference between these two kinds of attacks: direct attacks against IT assets compromise their availability, integrity, and/or confidentiality, whereas indirect, or security-protection attacks do not directly cause harm but provide advantage for the attacker, typically compromise the TSF, and preparing the way for later direct attacks.
- "Indirect attacks" should be explained in adequate detail and in such a manner as to ensure the readers are not confused by anticipation of TOE implementation details.
- The Guide should also explain that security-protection attacks tend to come from two main sources, hostile (human) threat agents and poorly trained or careless administrators. Thus, they are likely to be unimportant in environments that do not contain these threat agents.
- Consider using the following words: "Deciding which security-protection threats are significant in a particular environment requires knowledge of the environment and is best done by the PP author and sponsor. Choosing the particular combination of technical and environmental requirements to counter a given security-protection attack is again the responsibility of the PP author, as is defending the adequacy of the choice. The degree of attention given to security-protection attacks will vary greatly depending on the desired level of effectiveness and TOE assurance."

4.3.25 (3.3.3, first paragraph, first sentence, and second paragraph, first sentence) These sentences, especially the first sentence in the second paragraph, directly contradict the following assertion from page 39, Part 1, Annex B paragraph 2.4(b) of ISO 15408:

Note that not all possible threats that might be encountered in the environment need to be listed, only those which are relevant for secure TOE operation.

Thus, the Guide recommends the inclusion of threats that may be irrelevant, causing PPs to contain unhelpful information.

Recommendation. Change the Guide to be consistent with the philosophy expressed in ISO 15408.

4.3.26 (3.3.3, first paragraph, last sentence, and second paragraph, last sentence) No such requirement exists in ISO 15408. Asking the PP author to distinguish between threats addressed by the TOE and threats addressed by the environment violates the general structure of PPs (by asking the author to include solution information in a section that is explicitly intended for problem statement.

Furthermore, the form of this request conveys the view (also found in Version 1 of the CEM) that a given threat is likely to be countered by the TOE or by the environment. Rather, most threats are countered through coordinated effort by the two. Interestingly, this need for joint effort is found already in threats that were specifically chosen to show off the utility of ISO 15408 functional requirements, as will be seen from a detailed examination of the countermeasures presented at:

[
http://niap.nist.gov/TnC%20HTML%201/Catalogue%20Queries/Query%20Matrix%20.html]

Examination of ISO 15408-2 shows why co-ordination is indeed needed. Some ISO 15408 components assume communication with IT components in the TOE environment. Most ISO 15408 components have a suggested dependency on the management components, explicitly acknowledging dependency on the non-IT environment.

This request to classify threats discourages PP authors from carefully examining the necessary interplay between technical and procedural security measures by pretending that it doesn't exist.

Recommendation. Replace this guidance with the following empirically validated observations:

"Most threats cannot be adequately countered without coordinated effort between the TOE and its environment. This need for joint effort is implicitly found within ISO 15408 itself. Some Part 2 components assume communication with IT components in the TOE environment. Most components have a suggested dependency on the Part 2 management components, implying dependency on the non-IT environment. "

4.3.27 (3.3.3, next-to-last paragraph, first sentence)

Recommendation. Revise this guidance to be consistent with that suggested above.

4.3.28 (3.4) This section assumes that the organisational security policies are fully specified at the time that the PP is written. This is not always the case. For example, the PP may be written early in a system's life cycle, before some or all policies have been specified. It may be sufficient to specify the areas authors anticipated would be addressed by the policies without being able to specify the exact policies.

Recommendation. Add a discussion to this section that deals with the development cycle of the system and the policies it supports, so that the PP author can build in for the area anticipated to be addressed by evolving policies.

4.3.29 (3.4, para 3, sentence 1) This sentence is correct only for the limiting case of an organisation whose actions are carried out solely by machines with no possibility of

human involvement. This sentence leads to confusion between OSPs and TSPs because the distinction between OSPs and TSPs supplies the necessary basis for understanding how to balance technical and procedural security measures.

Recommendation. Replace this explanation with something that is consistent with ISO 15408's definition of Organisational Security Policy.

4.3.30 (3.4, para 3, last sentence) This statement is not true in all cases. If a PP is required to implement an organisational policy, then there is value in presenting that organisational policy in the PP, even if the PP authors have been so astute as to point out threats that are countered by the policy.

Recommendation. Soften or delete this advice.

4.3.31 (3.4, paragraph beginning "This security policy does ...") Organisational policies do frequently specify solution techniques for identified threats. The Guidance given should be sensitive to this fact of life.

Recommendation. Use the following advice instead of that given:

Organisational policies do frequently specify solution techniques for perceived threats. When a PP is obliged to include a policy that specifies solution techniques or compliance levels, the PP author has two choices. One is to present the policy in the environment section and reference it later in the Objectives section. The other is to recast the policy in a problem-solution format (if feasible), present the "problem" portion in the OSP section, and present the "solution" portion in the Objectives and/or Requirements sections. In the latter case, some convention is needed for clearly indicating that some objectives or requirements are included, as a matter of policy, with forward pointers from the PP's policy section to these objectives and requirements.

4.3.32 (3.4, paragraph beginning "As a general rule ...") Actually, the most difficult requirements to justify on the basis of threats are the detailed auditing requirements. Even the basic level of audit forces the collection of information that is not related to any obvious attack scenario.

Recommendation. Include Auditing as the first, most prominent example here.

4.3.33 (3.5.1, para 1) The second sentence is stated categorically, and it shouldn't be. There is good reason to believe that some PPs will find it desirable to distinguish threats, policies, and/or assumptions that apply only to the TOE or to a component in the TOE environment. Evaluators could use this paragraph as an excuse to cause trouble for a perfectly fine PP. Furthermore, the first sentence is not obvious and needs explication. Not only that, it's convoluted.

Recommendation. Recast this paragraph as follows:

Since the purpose of the Environment section is to cast the security problem to be addressed, the question of what the TOE does should not unduly influence the description of the environment. However, the environment may well contain IT components with which the TOE is assumed to interact. The enumeration of such IT components will clearly have a strong influence on what is left for the TOE to accomplish. ...

4.3.34 (3.5.2) There is some confusion as to which type of TOE comes first. Do the composite TOE or the component TOEs come first? If the component TOEs come first, are there any special considerations regarding the writing of a composite in the future?

Recommendation. Provide insight into the consideration necessary when composing systems.

4.3.35 (3.5.2, para 2, last sentence) The use of the word ”onto” here is not immediately obvious and deserves clarification.

Recommendation. Specifically, point out that if one TOE is a component of a second TOE, then the environment of the first TOE (directly or indirectly) includes the environment of the second TOE (and the environment descriptions for the corresponding PPs must be consistent with this fact.

4.4 - Section 4, The Security Objectives

4.4.1 (4.1, para 2, item (a)) Equating response and solution causes the purposes of the Objectives and Requirements sections to overlap. This may force unnecessary information into the Objectives section.

Recommendation. Replace this paragraph with a discussion of the difference between response and solution. Basically, the idea of the Objectives section is to identify the responsibilities of the TOE (response), not to specify TOE requirements (solution).

4.4.2 (4.1 second paragraph) There is only one aspect; the fact that it should be concise is just a suggestion.

Recommendation. In addition to the recommendation above, revise this section to clarify ”a concise statement of the intended response”, rather than confuse the issue with redundant statements.

4.4.3 (4.2, para 1, item (b)) The word ”satisfied” is used where ”addressed” is correct. The problem here is that PPs should have the flexibility to specify objectives in such a way that a given OSP is satisfied only through a combination of several different objectives.

Recommendation. Replace ”satisfied” with ”addressed.”

4.4.4 (4.2, para 2, last sentence) The Objectives should do something different from repeating the threats and OSPs, not something more than this. Don’t encourage excess specification.

Recommendation. Replace ”more than” with ”different from.”

4.4.5 (4.2, para 2) Use of the word how in this sentence echoes the previous error of expecting solutions in the Objectives section. By digressing into solutions, the Guide fails to provide any real guidance on what’s really needed here, thereby leaving PP authors in the dark. In fact, the Guide needs to explain that there are different levels of threat-countering intensity and different ways to counter threats.

Recommendation. Replace ”how” with ”the extent to which” and add the following guidance:

Objectives need to determine (to the extent desired by the PP author) what the responsibility of the TOE is in countering threats and in supporting organisational security policies.

Threat-countering objectives should clarify the kind of threat-countering measures the TOE will be involved in. There are three main kinds found among ISO 15408’s functional components:

- Preventive measures prevent a threat from being carried out or limit the ways in which it can be carried out. Access control measures tend to serve this purpose.
- Identification measures determine that a threat is being carried out. Audit and intrusion-detection measures tend to serve this purpose.
- Corrective measures limit damage after a successful threat has occurred and/or counter similar future threats. Data-integrity measures tend to be of this form, as are requirements for recovery to a secure state. Corrective measures are also referred to as recovery measures.

Normally, objectives are achieved only with a level of confidence less than absolute certainty. Thus, at least it is appropriate for the Objectives to informally quantify the minimal effectiveness expected. Several approaches to providing such quantitative information are possible. Quantities may be stated, (a) relative to other products, systems or environmental conditions, (b) relative to a previous situation, or c) via absolute numeric quantities. Approach c) is the most precise but also the most difficult to assess. The following three examples illustrate the above three approaches to quantification:

- Example (a): Objective for Protection of Life. Loss of life resulting from TOE-related threats is to occur no more frequently than from other causes encountered by TOE users.
- Example (b): Objective for Provision of Service. On average, loss of service resulting from TOE-related threats is to be less frequent, of shorter duration, and with milder consequences than losses of service that result from a failure to employ the TOE.
- Example c): Objective for Investigation of Failure. When loss of life or other severe loss does occur, identification measures shall have collected enough information to fully understand what caused the loss, in at least 85% of the incidents encountered.

The above examples also illustrate distinctions among, prevention, identification, and recovery. Example (a) clearly aims at prevention. Example c) explicitly aims at identification. Example (b) could be handled with any appropriate combination of prevention and recovery.

Note that a key feature here is that the objectives may directly or indirectly reference threats or other environmental statements. This fact has a significant impact on how the PP's Rationale must demonstrate satisfaction of objectives.

A well-written Objectives section will tell the reader how effective the countermeasures are for each identified threat, whether it is to be prevented, identified, and/or recovered from, and what role the TOE plays in doing this.

A well-written Objectives section that provides the above kinds of information leaves little doubt as to what level of effectiveness must be justified in the PP's Rationale section. If the PP fails to provide such information, then judgements about acceptable effectiveness are at the discretion of the PP's evaluators, which is something that the PP author may wish to avoid.

4.4.6 (4.2, last para on page 22) This paragraph gives good advice despite mixing objectives and requirements. The "objectives" suggested in this paragraph serve a different but legitimate purpose, namely that of organising the Rationale.

Recommendation. Refer to these as lower-level objectives in order to emphasise their differing purpose. Provide the following guidance on their use:

”Depending on the organisation and style of the PP, such lower-level objectives may overlap the higher level objectives used to define the TOE’s responsibilities. Alternatively, lower-level objectives may be introduced solely to facilitate the Rationale, in which case it may be more appropriate to present these lower-level objectives in the Rationale section.:

4.4.7 (4.2, example beginning ”The TOE must ...”) One of the great puzzles in ISO 15408 is to figure out whether a given objective should be categorised as for the TOE, for the environment, or both. Part of the problem is that an arbitrarily selected objective (in the ordinary English sense of the word) is most likely to be both. Such objectives not only hinder the goal of identifying TOE responsibilities but also run into an interesting piece of advice from ISO 15408:

”Note: when a threat or organisational security policy is to be covered partly by the TOE and partly by its environment, then the related objective shall be repeated in each category.”

Unfortunately, many objectives, including the single remaining example presented in this version of the Guide, meet the above criteria for duplicate listing: Unique identification normally depends on user protection of authentication data and, for those users who have stumbled on to other users authentication data, correct presentation of identity as well. It also depends on a correct administratively determined association between users and their initial passwords.

Recommendation. Provide guidance on what types of environmental dependencies may be safely ignored when failing to categorise an objective as ”for the environment,” using examples from the deleted Table (e.g., O.LABEL was an example of a pure TOE-only objective). Here is a suggested rule of thumb:

An objective need not be listed as for the environment, if it is met primarily by the functionality and assurances provided by the TOE. Some environmental support may be required, so long as this support is not explicit to the particular TOE objective and is obtained by meeting the environmental security objectives.

Whether a TOE objective is listed as ”for the environment” should depend partly on how it is mapped to the requirements. For example, the above I&A objective makes more sense as a TOE-only objective if biometrics are used, so that no specific user requirements are associated with fulfillment of the objective. If specific user requirements are needed to implement the objective (e.g., protection of passwords), then I.O&E looks more like a ”joint” objective that needs to be listed as both ”for the TOE” and ”for the environment.”

Finally, provide the following factual observations:

If there are many such duplicate objectives, then a PP author may prefer to use a more efficient method of listing joint objectives. One possibility is to provide a single list of objectives where each objective in the list is explicitly labelled as ”for the TOE” or ”for the environment.” Another possibility is to present three separate lists, one for the TOE, one for the environment and one for both the TOE and the environment.

4.4.8 (4.2, paragraph beginning ”It will be noted that ...”) This paragraph is too TCSEC specific! One of the main motives for moving away from the TCSEC was to free designers from the misconception that there are two main classes of polices (MAC and

DAC), as opposed to a vast space of possible policies, of which traditional MAC and DAC are merely two data points.

This paragraph detracts from the fact that in a typical TOE, there is always just one composite policy. In a given TOE, either a given access is allowed or it isn't, and the decision is always expressible in terms of composite criteria about the object and various entities in its environment (subject, user, time of day, etc.).

Recommendation. Delete this paragraph.

4.4.9 (4.2, paragraph beginning "The CC requires ...", third sentence) Placing the same mapping in both the Objectives section and in the Rationale creates undesirable bulk, not to mention a maintenance problem.

Recommendation. Recast this sentence to advocate the possibility of putting the mapping, e.g., in the Objectives section, with a pointer or reference to it from the Rationale section.

4.4.10 (4.3, first sentence) This sentence does not correlate with item c) in the following paragraph.

Recommendation. Replace "satisfied" with "fully satisfied."

4.4.11 (4.3, first paragraph beginning "The statement of security objectives...") As already noted, the proposal to represent detailed requirements for the non-IT environment as "Objectives" sets up an artificial lack of parallelism between IT requirements and non-IT requirements. ISO 15408 provides no support for this asymmetry. Indeed, it explicitly discusses requirements for the non-IT environment in ISO 15408-1, Annex B.2.6 (b), describing them as "often useful in practice." This mistreatment of requirements as objectives appears to result from an attempt to shoehorn all PPs into the incomplete structure of Figure B.1 Part 1, Annex B.

Whatever the motivation, treating non-IT requirements as objectives may leave the PP author with inappropriate choices. PP authors are either mixing requirements in with objectives (contrary to the intent of the Objectives section) or else omitting non-IT requirements altogether, in hopes that implementers and TOE evaluators will rediscover them on their own. The importance of this issue stems from observations given above on the need for co-ordination between the TOE and its non-IT environment.

Recommendation. Don't confuse objectives with specific usage requirements such as protection of passwords. Instead, explain the following:

Most security services need to be managed in order to be effective. Sometimes, the required management activity is obvious and may conveniently expressed via a high-level non-IT objective (e.g., regarding the need for proper management of audit functions). Other times, the required management techniques depend nontrivially on the particular threats to be countered or on the detailed requirements used to implement TOE objectives. For example, an authentication objective may be implemented with ordinary user passwords, leading to a low-level user requirement to protect password secrecy.

4.4.12 (4.4.1, Title) The more general concern that might be addressed here is dependencies on the environment - both IT and non-IT.

Recommendation. Generalise this section so that it is more consistent with the needs of PP authoring. Specifically, explore the use of non-IT objectives and requirements in support of TOE objectives. Give examples, e.g., a TOE objective is to perform I&A, but

this is unlikely to happen without proper administration, even if the best biometrics I&A techniques are employed. Note that the second paragraph, in particular, generalises without significant modification.

4.4.13 (4.4.1, first paragraph) The word ”satisfied” is twice used where ”addressed” is correct. ISO 15408 does consider the case where a given objective is to be met partly by the TOE and partly by the environment. A previous comment explains why this is important - a given threat may be addressed by any combination of technical and non-technical measures.

Recommendation. Replace ”satisfied” with ”addressed.”

4.5 - Section 5, IT Security Requirements

4.5.1 (5.1) Some readers might naively assume that this section is about the TOE.

Recommendation. Add the following sentence to the first paragraph: ”This guidance applies to both TOE requirements and to requirements for the IT environment.”

4.5.2 (5.1, last para on page 26, first sentence) Any component can be refined, so a degree of flexibility is allowed for any component.

Recommendation. Delete ”, for some functional components defined in [CC2], ”.

4.5.3 (5.2.1, page 23, first paragraph) The Guide should also point out that dependencies should be applied in a consistent fashion.

Recommendation. Say the following:

Dependencies should be applied in a consistent fashion. For example, in the case of FAU_ARP.1, consistency is ensured by the nature of the requirements (FAU_ARP.1 relies on the expectation of a potential security violation that is defined by application of FAU_SAA.1.2.

For other components, consistency may be more problematic. In the case of FDP_ACC.1, the PP is likely to specify a particular access control SFP (since the requirement is otherwise vacuous). At this point, the applied FDP_ACC.1 should normally depend not on FDP_ACF.1 itself but on the corresponding application of FDP_ACF.1 to the same access control SFP that was used for FDP_ACC.1.

4.5.4 (5.2.1, page 23, first paragraph, item (b); page 24, first paragraph) This sentence gives the impression that the decision to add additional supporting requirements is entirely at the discretion of the PP author, which is not necessarily the case.

Recommendation. Explicitly relate this activity to security-protection threats, as discussed above. Specifically, explain that having added a security function, it may then be necessary to protect that function from composite attacks that first defeat the function, then mount the threat the function was designed to counter.

4.5.5 (5.2.1, page 24, item (b)) This example seems to say that things like FPT_AMT.1 and FPT_SEP should generally be tossed into PPs, without any explanation of why or when. To avoid unmotivated subjectivity, it is important that these requirement be tied to threats, policies, and/or explicit TOE effectiveness objectives. For example, a quick search of the database at:

[
http://niap.nist.gov/TnC%20HTML%201/Catalogue%20Queries/Query%20Matrix%20.html]

suggests the following security-protection attacks as possible motives for including FPT_AMT.1:

- Undetected TSF Failure
- Undetected Modification of TSF Hardware
- TOE-Related Corruption of TSF
- Inadvertent TSF Self-Modification
- Install Malicious Logic (by user)
- Install Malicious Logic by Administrator
- Install Malicious Logic during Delivery
- Install Malicious Logic during Development

Expressed concern for these kinds of threats in the PP itself would clearly justify the inclusion of FPT_AMT.1. Pointing this out in the Guide will discourage PP evaluators from demanding inclusion of FPT_AMT.1 just because the Guide recommended its inclusion without qualification.

Recommendation. Recast Item (a) as follows:

a) SFRs such as FPT_AMT.1 (Abstract Machine Testing) and FPT_SEP (Domain Separation) may be needed to support the PP's security objectives if these SFRs help counter-identified security-protection threats (e.g., TSF failure, corruption, or modification, possibly by malicious means).

4.5.6 (5.2.1, page 30, item (a)) The example is a bit one sided. If the data is collected, as per FAU_GEN.1, it should normally either be reviewed or else exported to some other system for review.

Recommendation. Generalise the example to cover both possibilities, namely review and export.

4.5.7 (5.2.1, page 30, first para following list at top of page) Adding more requirements just to get a different PP is a bad idea.

Recommendation. Modify the paragraph to mention the addition of additional threats, policies, and/or objectives as well.

4.5.8 (5.2.1, last para, last sentence) This sentence seems to indicate that PPs always get bigger.

Recommendation. Replace ”additional SFRs” with ”different SFRs” to avoid reinforcing the assumption that PPs always get bigger.

4.5.9 (5.2.2, page 25, first full sentence) This sentence echoes the error previously noted. At the expense of possible awkwardness, it is always possible in principle to explicitly formulate the composite policy enforced by a system.

Recommendation. Replace ”it may be necessary” with ”it may be desirable.”

4.5.10 (5.2.2, page 25, paragraph beginning ”The choice as to whether ...”) Individual PP authors are not the only individuals who have a stake in whether requirements are over-specified due to excess application of assignment and selection operations. Over-specification causes the bloating of PP Registries by encouraging the proliferation of multiple PPs that all serve basically the same purpose. Over-specification also artificially reduces the class of products that may legitimately meet the PP's requirements, even though they meet the PP's objectives and should thus have been

considered compliant. Consequently, two key issues here are bloated registries and economic unfairness caused by overly restrictive requirements.

Recommendation. Rewrite this paragraph to include strong advocacy for avoidance of unnecessary detail. In support of this advocacy, introduce the concept of partially completed operations:

”A PP may contain any combination of completed operations and uncompleted operations. In addition, it may contain partially completed operations where some of the possibilities for applying an operation have been eliminated but not all of them. For example, suppose there is an operation to specify allowed password length and the PP says ”at least 4 characters, but possibly more, depending on whether control characters are allowed.” This is a partial application of the operation, since the ST author is free to specify a minimum password length of 4, of 5 printable characters, or of 23 for that matter. In general, the PP author should pass on as much as is known about how to fill in an operation but no more.”

ISO 15408 does not discuss the notion of partially completed operations, but there is a clear need for them, they do not contradict anything in ISO 15408, and several ISO 15408 authors have stated they are useful.

4.5.11 (5.2.2, page 25, paragraph beginning ”Completing the operations ...”) ISO 15408 discusses completeness of operations but does not provide explicit guidance on what constitutes completeness. This has proved to be a problem in reviewing PPs. (One PP author claimed completeness meant syntactic completeness and just rephrased each component in such a way as to make its ”T.B.D.s” not obvious.)

Recommendation. Explain completeness of operations. The intent (inferred from examples in the Annexes of ISO 15408-2) is this:

An operation has been completed when the implementer has been told how to proceed. That is, the implementer has either been told what decision has been made or has been told to support runtime decision-making.

4.5.12 (5.2.2, page 25, paragraph beginning ”If an operation is ...”, second sentence) This sentence appears to imply that ISO 15408 components included in a PP should be included by copy as opposed to by reference. Such a stylistic constraint is particularly bad for PPs written in HTML, where a hyperlink may be the most convenient and accurate method of inclusion.

Recommendation. Recast this sentence as ”For example, FDP_RIP.1.1 could be included, either directly or by reference, as: ...”

4.5.13 (5.2.2, page 25, paragraph beginning ”Where assignment or ...”) Nice example.

4.5.14 (5.2.2, page 26, next-to-last para) This is not simply an example of a refinement. The original element constrains arbitrary secrets, whereas the ”refinement” constrains only passwords, in potential contradiction to the constraint that refinements restrict implementations. However, the given requirement may be justified through creative application of assignment, refinement, and possibly iteration:

- [Iteration: If FIA_SOS.1 has already been used in the PP, start with fresh copy.]
- Assignment: Use the metric ”if it’s a password then it has at least 8 characters” (the metric applies to all secrets, but vacuously to non-password secrets).

- Refinement: the TSF shall enforce a minimum password length of 8 characters" (simplifies the result of the previous step (this is a trivial form of refinement)

Recommendation. Suggest using a different example. If this example is used at all, it should be treated much more carefully, as above.

4.5.15 (5.2.3, first three paragraphs) The first two paragraphs unambiguously convey the mis-impression that if auditing is used, then auditing must be specified via the minimum-basic-detailed mechanism provided in ISO 15408.

Recommendation. Recast the first two paragraphs in such a way that they do not contradict the third.

4.5.16 (5.2.3 re: minimum, basic, or detailed) The different levels need to be compared. Developers of PPs and STs will be looking for help in identifying and quantifying these types of varying categories.

Recommendation. Some text should be added here to compare and contrast these three levels.

4.5.17 (5.2.3, last paragraph) Good advice. Keep this!

4.5.18 (5.2.4) Unfortunately, specific guidance cannot yet be proposed regarding FMT. However, it is evident that ISO 15408 is quite vague about which management functions are relevant to a given non-management component.

Recommendation. Hopefully, somebody will have time to work through a suggested mapping that takes each non-FMT component to those FMT components that are likely to be relevant.

4.5.19 (5.2.5, second para) Good guidance! Keep it.

4.5.20 (5.2.5, third paragraph) The Guide should discuss the extent to which it is advisable to model new SFRs on existing components, families, or classes.

Recommendation. Say the following:

Knowing that a new SFR is of similar nature to others in an existing class or family helps bound its degree of newness and also may help with specific wording for common concepts that occur throughout that class or family.

4.5.21 (5.2.5, fourth paragraph) A third stylistic characteristic of ISO 15408 elements is that each element tends to stand on its own and can be understood without reference to previous elements.

Recommendation. If the Guide authors agree, add this point to the list.

4.5.22 (5.2.5) The SFRs that are not included in ISO 15408-2, but are developed for inclusion into a PP, should be considered for inclusion into the next iteration of ISO 15408-2.

Recommendation. ISO 15408-2 is only as good as the combined knowledge of its authors for any particular iteration. Including a statement similar to the following will add to PP and ST authors motivation to be clear, concise, and accurate when developing or refining SFRs.

A PP or ST author who believes they have a well constructed SFR; that is not included in, is significantly different than, and would significantly enhance, the existing SFRs in

ISO 15408-2, is advised to submit the SFR for inclusion in the next iteration of that document.

4.5.23 (5.2.5, last paragraph) A fourth consideration is the management implications of the SFR.

Recommendation. Add a reference to FMT.

4.5.24 (5.2.5, general)

Recommendation. Point out the following:

For reasons of PP maintainability, short names for SFRs not in ISO 15408 should not conflict with future ISO 15408 class, family, and component names. There are many ways to do this: use hyphens instead of underscores, include a numeral, a question mark, etc. Just don't make them of the form AAA_BBB.

4.5.25 (5.2.6) This well-presented section contains great advice!

4.5.26 (5.3&5.4.4) The reference to the Evaluation Assurance Level (EAL) is by name alone.

Recommendation. Reference clause 6 of ISO 15408-3 for further guidance on EALs.

4.5.27 (5.3, first para, item (f)) Item (f) is not directly a reason for choosing an EAL, as the reasonable alternative is to accommodate the dependency through the use of an augmented EAL.

Recommendation. Delete item (f) and instead discuss dependencies under augmentation in the following paragraph.

4.5.28 (5.3, last para, last sentence) The sentence is incorrectly worded. Augmenting EAL3 with AVA_VLA.4 is not necessarily inappropriate if the augmentation also includes ADV_LLD.1 and ADV_IMP.1.

Recommendation. Recast as follows:

For example, if a PP augments EAL3 with AVA_VLA.4, then it should also augment with ADV_LLD.1 and ADV_IMP.1, as these are not included in EAL3.

4.5.29 (5.3.X)

Recommendation. Discuss non-ISO 15408 assurance requirements in a PP, even if only to acknowledge their existence.

4.5.30 (5.4.1, first two paras) Good.

4.5.31 (5.4.2) Good.

4.5.32 (5.4.X)

Recommendation. Discuss non-ISO 15408 assurance requirements in an ST.

4.5.33 (5.5.1) The pursuit of generality represented here is both admirable and appropriate.

Recommendation. Do not sacrifice this goal.

4.5.34 (5.5.1) The presentation in this section is confusing and could be organised better. The supposed "problem" mentioned in the first sentence is not explicitly identified, and it has little to do with whether the requirements are expressed as SFRs. Items, (a) and (b), in the first paragraph are presented as presentation options when in

reality they are mutually exclusive cases that do not arise in the same PP. Furthermore, there are really three cases that need to be discussed.

Recommendation. Reorganise the presentation along the following lines:

- Case A. The division of responsibility between the TOE and environment is fully determined: Specify environmental requirements in their own section(s), using multiple sections if there are multiple environmental components that need to be specified. (ISO 15408 doesn't explicitly recommend multiple subsections for environmental requirements, but it does explicitly make the analogous recommendation for threats, policies, and assumptions [Part 1, Annex B.2.5, last para]; the same reasoning obviously applies here.)
- Case B. The division of responsibility between the TOE and environment is not fully constrained by the PP, but the requirements can be stated the same way, independently of whether they are satisfied by the TOE or by the (IT) environment. Proceed as in Case A, adding additional subsections covering sets of components, any one (or more) of which may implement the requirement. Alternatively, put all IT requirements in the same section, title it "IT Security Requirements" rather than "TOE Requirements" or "Requirements for the IT environment", and explicitly identify which requirements may be satisfied by which components. (This sub-option breaks with the non-normative Figure B.1, but for good reason.)
- Case C. The division of responsibility between the TOE and environment is not fully constrained, and the statement and meaning of a given requirement varies somewhat depending on where it is implemented. This is best handled through the use of parameterised PPs, a topic that may be outside the scope of the Guide.

4.5.35 (5.5.1, para 2, sentence 2) This is good motivation for considering Cases B and C above. Keep this point.

4.5.36 (5.5.1, last paragraph on page 30) This is part of the confusion. See earlier comment.

4.5.37 (5.5.1, first paragraph at top of page 31) Great point, keep it!

4.5.38 (5.5.1, next-to-last para) The need to provide dependencies at a more abstract level may arise independently of whether there are environmental requirements or whether the role of the environment is not fully pinned down (although these factors may promote uncertainty an thus the need for abstract dependencies.

Recommendation. Generalise this discussion and place it in Section 5.2.1, where it will be more easily comprehended.

4.5.39 (5.5.1) As explained already, there may well be a need for a PP to include requirements for the non-IT environment.

Recommendation. Include a discussion of requirements for the non-IT environment, either here under dependencies or in a separate subsection titled Optional Requirements for the Non-IT Environment. Include at least the following points:

Requirements for the non-IT environment are needed in a PP when there are non-IT objectives whose implementation is not straightforward or when the rationale depends explicitly on how the non-IT objectives have been realised. The latter case arises when there is a need for detailed co-ordination between the PP's requirements and

associated management techniques, with the two kinds of requirements being at a similar level of abstraction.

Rather than mix abstraction levels by treating non-IT requirements as objectives or assumptions, it is better to provide a separate section for non-IT requirements. Such a section might cover such topics as the protection of authentication data used by a particular I&A mechanism (e.g., passwords), as well as specific administrative requirements (e.g., investigative procedures needed in response to various intrusion-detection alarms).

Providing a clear identification of known non-IT requirements in the PP ensures that these requirements will reliably propagate into user documentation - assuming that the appropriate documentation requirements from Class ADO are included in the PP.

4.5.40 (5.5.1, last para) In the happy event that all products are evaluated products, and in view of the fact that products are increasingly interdependent, this piece of advice implies that all products will be at least equal to the most highly assured products. Obviously, the conclusion doesn't hold. For example, it would be highly inappropriate to expect every PC in the environment of a certification authority to have as much assurance as the Certification Authority.

Recommendation. Replace this para with the following observations and guidance:

Pragmatic considerations in the design of large multi-component systems demand that high-assurance components be minimised, due to their increased cost. The general philosophy is to isolate the information that needs the most protection into a few high-assurance components (e.g., isolate the root keys held by a certification authority).

4.5.41 (5.5.2, 2nd line) It appears that the authors made a typo.

Recommendation. This should read "and does not need"

4.5.42 (5.5.2, first para, last line) ISO 15408 does not support the association of an assurance level with individual SFRs.

Recommendation. Recast to avoid this misimpression.

4.5.43 (5.5.2, second para) This is a good example of including documents (and their requirements) by reference. This example supports comments made earlier regarding the need for a referenced-documents section in PPs.

4.5.44 (5.5.2, paragraph beginning "It may be noted ...", last sentence) The assertion is false as stated.

Recommendation. Fix by adding "in high-risk (local) environments" to the end of the sentence.

4.6 - Section 6, the TOE Summary Specification

4.6.1 (6.1, Item (b) in second list) This particular recommendation tends to be unclear.

Recommendation. An example here would be very helpful to the reader's understanding.

4.6.2 (6.2, second para) The previous material in Section 6 suggests that the TOE Summary Specification exist for ease of understanding. Either the preceding paragraphs have left out something important or else there need not be any new information provided (assuming that the SFRs are easy to understand. Nothing in ISO

15408 or in the preceding portion of Section 6 suggests that more detail is necessary for all PPs.

Recommendation. Recast the first two sentences as follows: ”Those IT security functions which specify the principal security purpose of the TOE should receive the most detailed attention.”

4.6.3 (6.3, last para) This is a useful introductory sentence.

Recommendation. Put this at the beginning of 6.3 or even sooner.

4.6.4 (6.4, para 2) This section is very hard to read. The first sentence says, ”the evaluation itself will confirm whether the assurance measures are sufficient to satisfy the assurance requirements”. The second sentence seems to contradict the first by saying, ”the evaluation of the ST will not be able to prejudge whether or not the assurance measures are sufficient to meet the assurance measures”. It appears that the same evaluation is being talked about. If that is the case, then the paragraph doesn’t make sense.

Recommendation. If the first sentence was changed to say, ”the TOE evaluation itself...”, then the paragraph’s meaning is easily relevant.

4.6.5 (6.4, para 2) The presence of this paragraph comes as a surprise, as no similar statement was made in connection with functional requirements. This difference in treatment leaves the reader with the unanswered question ”Why the difference?”

Recommendation. Please explain.

4.6.6 (6.5.1, Dependencies) The dependencies on the IT environment are in principle no different from dependencies on the non-IT environment. Exactly the same issues arise.

Recommendation. Generalise the discussion to accommodate both kinds of dependencies. Include a non-IT example, e.g.:

The PP might specify authentication and user protection of authentication data, whereas the ST might specify passwords and user protection of these. The refinement of the TOE requirement obviously carries over to a corresponding refinement of the usage requirement and should show up in the TOE’s user documentation.

4.6.7 (6.5.1, second para, last sentence) The example is confusing in its present form. What is meant or implied here with the use of syslog()? This is too detailed an example.

Recommendation. Recast so that the example is explicitly about the environment or provide more justification for using syslog():

The ST assumes that audit data is exported to an environmental component that understands Unix syslog() format.

4.6.8 (6.5.1, last para, first line) Not all TOEs have underlying platforms.

Recommendation. Replace ”the TOE” with ”a software TOE”.

4.6.9 (6.5.2) The reference to ”IT Security Requirements” makes sense only in the ”Case B” situation discussed above.

4.7 - Proposed Section on PP Application Notes

4.7.1 Not much guidance on application notes has been collected. However, it appears that some PP authors prefer to scatter their application notes throughout the PP rather than collecting them in a single section.

Recommendation: In any case, there is an obvious need to co-ordinate individual application notes with other portions of the PP that they happen to be about. It may be possible to collect all of the application notes into a single section without the use of hyperlinks.

4.8 - Section 7, PP Rationale

4.8.1 (7.?) The approach suggested for identifying and explaining completed operations is only one possibility. The rejected alternative of identifying them in the rationale may be preferable in some circumstances. For example, the PP minus its rationale may be part of a contract. It would be confusing and inappropriate to include explanation of completed operations in the contract.

Recommendation. Look at alternative approaches, for identifying and explaining completed operations, that might be applicable especially in relation the above and add discussions as appropriate.

4.8.2 (Figure 6) The figure does not reflect the relationship between the IT Security Requirements and the Security Objectives, nor does it talk about them in any detail.

Recommendation. Add lines from the IT Security Requirements to the Security Objectives to indicate the proper relationship and add additional paragraphs to sufficiently discuss that relationship as per ISO 15408.

4.8.3 (7.1, para 2) This paragraph distorts the intent of the Rationale, as expressed in 15408-1, Annex B, by omitting the requirement to show that ”a conformant TOE would provide an effective set of IT security countermeasures within the security environment.” By simplifying the task to showing that the requirements satisfy the stated security problem, this assertion leaves out the PP’s stated response to the security problem, as defined in the PP’s Objectives section.

Recommendation. Recast this paragraph so that it is consistent with 15408-1, Annex B.

4.8.4 (7.1, para 2,) The Guide replaces suitability with satisfy and security environment with security needs . This differs from ISO 15408-1 B.2.5(a) and (b) , which refer to countering threats and meeting OSPs and assumptions. Making use of multiple terms to describe the same thing leads to massive confusion. It appears that the Guide may supplant or replace the PP author’s right to specify the PP’s response to the environment with the PP evaluator’s opinion of what these vague words might mean.

Recommendation. Define the new terms as to their relationship with ISO 15408 terms or use ISO 15408 terms and further describe suitability not as addressing, satisfying, countering, meeting, or achieving, but as making a well-defined, suitable response along the lines discussed above in connection with PP objectives.

4.8.5 (7.1, para 2) Clearly, suitability or as stated in the Guide ”satisfy” must be interpreted differently for requirements than for objectives, since the PP’s stated response to the environment has already been taken into account.

Recommendation. Define suitability of requirements to mean that the combined set of IT and non-IT requirements together satisfies all of the objectives, where the non-IT

requirements need not occur explicitly in the PP but may simply be evident from the non-IT objectives.

Explicitly point out the possible need to include non-IT requirements in the PP:

If non-IT requirements are needed that are not obvious from the non-IT objectives, and if these non-obvious requirements are not contained within the PP, then it may be infeasible to demonstrate suitability of the IT requirements.

4.8.6 (7.1, last para on page 37) Good guidance.

4.8.7 (7.2, first para). For a PP of any size, either Item (a) or Item (b) of the last assertion in this paragraph will be false! If the table lists objectives down the first column and environmental statements in the second, then it should be obvious that each objective addresses at least one environmental statement (i.e., threat, OSP, or assumption). The converse need not be true because it may take quite awhile to search the table for each environmental statement (security need - see comment above about terminology) to be sure that it's there. Similarly, if the table is organised with environmental statements (security needs) down the first column, then it may take quite awhile to be sure each objective occurs in the table. Finally, if the table is organised as a bit matrix (e.g., objectives across the top and environmental statements (security needs) down the page), then both items might be obvious (but only if one has a very large page on which to display the matrix. Mercifully, only Item (b) of this sentence actually needs to be true. That is, it suffices to list objectives down the first column, since the environmental statements (security needs) must then be enumerated and discussed individually in any case.

Recommendation. Recast the first two paras as follows:

The Objectives Rationale must demonstrate two things:

- Necessity: each security objective addresses at least one environmental statement (security need) (i.e., at least one threat, organisational security policy, or assumption).
- Sufficiency: each environmental statement (security need) is addressed at a suitable level of effectiveness by the objectives.

To demonstrate necessity, it suffices to present a table or similar chart that maps each objective to the environmental statements it addresses.

To demonstrate sufficiency, it is typically necessary to list each environmental statement individually and argue that it is being addressed by conforming TOEs in intended environments of use in a manner that users and other stakeholders will find suitable.

Note that the above advice may need to be modified somewhat if the PP author includes lower-level objectives, as discussed earlier.

4.8.8 (7.2) In section 3.3, it is stated, "the Common Criteria does not provide a framework for risk analysis". This section deals explicitly with a large portion of an organisation's methodology for completing a risk analysis.

Recommendation. It is prudent that a footnote be placed here that might read:

This section only justifies the security objectives against the security environment and should not be represented as a full blown risk analysis, even though it contains statements that might be similar to statements in a risk analysis. It is up to the

individual organisation to define what is acceptable risk and to complete a risk analysis when revising or defining their security policy. Upon a favourable evaluation the PP or ST, a consumer/user might choose to use this section as a basis for argument in the organisation's risk analysis process.

4.8.9 (7.2, second para, second sentence) The implicit assertion that countering a threat is equivalent to preventing it is outmoded. This view is based on a risk-prevention paradigm popularised by the Orange book. Today, the preferred approach is risk management, in which not all threats are countered all of the time. As discussed earlier, countermeasures may be preventive, detective, or corrective in nature. In many cases, prevention is neither possible nor necessary. Consider a TOE that counters integrity threats arising from corrupt data arriving on a noisy channel. The TOE cannot prevent the threat, but it may be able identify and recover from it (and there's nothing wrong with the TOE because of that. It appears here that PP evaluators will disallow perfectly fine PPs just because they fail to support the now discredited notion of risk avoidance advocated by the Guide.

Recommendation. Change the sentence "...or that the likelihood of it occurring is reduced to an acceptable..." to "..., that the likelihood of it occurring is reduced to an acceptable level, or that instance of it occurring has been accepted in the OSP through risk management. Optionally, add some of the above discussion on risk avoidance and risk management.

4.8.10 (7.3.1, the Title) This section is about suitability of the requirements, not just about sufficiency of the requirements.

Recommendation. The Guide authors should either choose a more accurate title or else split this section into two separate sections dealing with necessity and sufficiency.

4.8.11 (7.3.1, first para) This paragraph has the same problems as (7.2, first para). This is most unfortunate. The demonstration of requirements sufficiency is the very heart of the rationale. The Guide should leave no doubt about the unacceptability of substituting rationalisations for rationale here. A very precise explication of sufficiency is needed here.

Recommendation. The solution is similar to that recommended in an earlier comment. Say the following:

To demonstrate suitability of the PP's requirements, it is necessary demonstrate two things:

- Necessity: each security requirement addresses at least one objective.
- Sufficiency: each objective is satisfied, given that the explicit requirements and inferred environmental requirements are satisfied. (The inferred environmental requirements are made obvious by the environmental objectives, even though they are not listed explicitly in the PP).

To demonstrate necessity, it suffices to present a table or similar chart that maps each requirement to the objectives it addresses.

To demonstrate sufficiency, it is typically necessary to list each objective and argue that it is satisfied, assuming that the explicit requirements and inferred environmental requirements are satisfied. In making this argument, it is important to take into account the following:

How and why ISO 15408 operations have been applied (especially in the case of access control requirements).

How dependencies are accommodated. For example, preservation of secure state (a functional requirement) depends on how secure state is defined (an assurance requirement).

How TOE requirements are coordinated with requirements for the TOE environment.

Note that the above advice may need to be modified somewhat if the PP author includes lower-level objectives. In this case, higher-level objectives may follow from any reasonable combination of lower-level objectives and/or requirements.

4.8.12 (7.3.1, page 38, para 2) APE_REQ.1.13 uses the phrase ”requirements are suitable to meet,” and the Guide substitutes the phrase ”sufficient to meet.” It appears here that PP authors and evaluators will genuinely not understand what it takes to prevent the creation of PPs whose requirements simply do not live up to the expectations established by the PP’s Objectives.

Recommendation. See earlier comment on this topic.

4.8.13 (7.3.2) What is the original basis for the EALs? That has not been made clear in any other documents.

Recommendation. Some reflection on the original basis of EALs (at least) should be included.

4.8.14 (7.3.2, para a)) It appears here that information on whether the TOE is intended to defend against sophisticated attacks may be found only in the Rationale section where only PP evaluators are likely to read it, so that consumers and TOE developers are left in the dark. This section needs to be expanded.

Recommendation. Explain which PPs have the property that ”the TOE is intended to defend against sophisticated attacks” and, for these, what kind of sophistication is anticipated. Also, explain the following:

This part of the Rationale has to be consistent with what the PP has had to say about security-protection attacks, as discussed earlier. This part of the Rationale also has to be consistent with what the PP’s Objectives have said about desired effectiveness, as discussed earlier. In particular, if the Objectives indicate a need for attention to strength of function considerations, then it is reasonable to expect that the assurance requirements will include AVA_SOF.1.

4.8.15 (7.3.3, both paras) This section confuses two different constraints:

First Constraint. If the PP includes AVA_SOF.1 then a uniform strength-of-function requirement shall be included in the TOE functional security requirements section of the PP, and in this case the uniform minimum shall be designated as SOF-basic, SOF-medium, or SOF-high. (This constraint is given in ISO 15408 Part 1, Annex B.2.6.)

Second Constraint. The PP must include sufficient strength-of-function requirements to meet its TOE Objectives.

It appears here that this section fails to emphasise that the second, more important constraint needs to be met whether or not AVA_SOF.1 is included.

This section also confuses the requirement to meet APE_REQ.1.12 with the need to provide a separate Rationale argument. There is no such need. If AVA_SOF.1 is in the PP, then most evaluators can probably scan well enough to see whether the TOE

Security Requirements include a uniform strength-of-function claim, which takes care of the First Constraint. If the Requirements Sufficiency argument is given correctly, then the Second Constraint will be met as well. It appears that the only reason for giving a separate strength-of-function argument is the PP has botched its requirements-sufficiency argument. To put it another way, PP evaluators should able to evaluate APE_REQ.1.12 when reading the PP's requirements-sufficiency argument, unless there's something already wrong with this argument.

Recommendation. Untangle the above confusions by making the following points:

There are two different ISO 15408 requirements concerning strength of function:

The PP must include sufficient strength-of-function requirements to meet its TOE Objectives.

If the PP includes AVA_SOF.1, then a uniform strength-of-function requirement must be included in the TOE functional security requirements section of the PP, and the uniform minimum must be designated as SOF-basic, SOF-medium, or SOF-high. (cf. ISO 15408-1, Annex B.2.6(a)(1)])

Evaluation Requirement APE_REQ.1.12 addresses both of these requirements. This evaluation requirement on the PP's rationale does not necessarily mean that a separate subsection must be devoted to strength of function in the PP's Rationale, provided the following criteria are satisfied:

The Requirements Sufficiency argument includes any strength-of-function arguments needed to ensure that the TOE Objectives are satisfied.

If AVA_SOF.1 is included, then the TOE Security Requirements explicitly include an appropriate uniform strength-of-function claim

Conversely, if the Objectives do indicate a significant need for attention to strength of function considerations, then the assurance requirements should probably include AVA_SOF.1.

4.8.16 (7.3.3) What is the original basis for the strength specifications in ISO 15408? That has not been made clear in any other documents.

Recommendation. Some reflection on the original basis for the strength of specifications in ISO 15408 (at least) should be included.

4.8.17 (7.3.4, para 2, Items (b) and (e))

Recommendation. First, delete the qualifier "if necessary," in Item (b), as necessity is clear from Item (e). Second, in both items, SFR is used where row would be clearer. Say "row."

4.8.18 (7.3.4, para 4) Good guidance.

4.8.19 (7.3.4, approx para 6) Version 0.6 of the Guide mentioned "internal consistency" where this version does not. Internal consistency is a prerequisite to mutual support.

Recommendation. The Guide should discuss consistency and give explicit recommendations on consistency. One good, traditional way to show consistency is to build a TOE that clearly satisfies all any security requirements whose feasibility is in doubt. Of course, the PP's Rationale would merely cite the existence of the TOE and any studies showing its satisfaction of the PP. Also, include or reference the advice in our proposed Section 4.3.4.

4.8.20 (7.3.4, paras 6-8) These interesting and instructive statements appear to be aimed at reviewers of the Guide rather than at ordinary users of the Guide.

Recommendation. Mark them as editorial notes to be deleted or replaced with a brief summary in the final version.

4.8.21 (7.3.4, para 8) This paragraph seems to be explaining the real contribution of the mutual support concept in terms of security-protection attacks. The specific types of security-protection attacks mentioned are bypassing security mechanisms, tampering with security mechanisms, de-activating security mechanisms, exploiting undetected mis-configurations, etc.

Recommendation. If the authors of the Guide agree with the above assessment, then be explicit about what is intended by this term (say the following:

If a security-protection attack can be used in preparation for a primary attack, then any requirement that counters the security-protection attack supports any requirement that counters the primary attack. Mutual support encompasses both this kind of support as well as the kind associated with ISO 15408 requirements dependencies.

4.8.22 (7.3.4, paras 9-13) This portion of the Guide is trying to do the same thing as the security-protection portion of the threats-and-countermeasures database at:

[
http://niap.nist.gov/TnC%20HTML%201/Catalogue%20Queries/Query%20Matrix%20.html]

Recommendation. Suggest augmenting the Guide with ideas from the above referenced database.

4.8.23 (7.3.5, last para) This seems to be in a different vein from other kinds of mutual support, and it is not really needed. As already pointed out, audit collection by itself doesn't pose much of a countermeasure (or sensible OSP). Thus, if FAU_GEN.1, for example, has come into the PP in response to some threat or sensible policy, it should already be coupled with other requirements that serve the same threat-countering or policy-serving objective. There is no need to redundantly make this point in conjunction with mutual support.

Recommendation. Delete the last paragraph in Section 7.3.5.

4.8.24 (7.3.4para 9) What is the connection of FPT_AMT.1 to this discussion?

Recommendation. The connection to FPT_AMT.1 should be clarified.

4.8.25 (7.4.2, first para, item (b)) This point is not obvious at best. It should be true only if each objective for the composite PP belongs to one (or more) of the component PPs.

Recommendation. Consider deleting this claim. Alternatively, explain why it's true.

4.9 - Section 8, ST Rationale

No Comment

4.10 - Section 9, Functional and Assurance Packages

No Comment

4.11 - Annex A, Guidance Checklist

No attempt has been made to identify the consequences for Appendix A of the comments on previous sections, as the necessary changes will, in any case have to await revision of the main body.

4.11.1 (A.1.2)

Recommendation. It is suggested that the first sentence start off with, ”To identify the relevant threats...”.

4.12 - Annex B, Generic Examples

4.12.1 (B.1, example threats) There is an inconsistency between the examples and the guidance in the earlier chapter. As specified in section 3.3.3: ”threats countered by the environment could be labelled TE1, TE2, TE3 and so on, with the ‘E’ signifying that the threat should be addressed by some means deployed within the TOE environment”. It should be noted that in accordance with guidance in ISO 15408-1 B.2.4(b), only the threats that might be encountered in the environment and are relevant for secure operation of the TOE need listed.

Recommendation. The second set of example threats should be changed to have ‘TE’ preceding the threat name.

4.12.2 (B.2 re: MAC policy) This example fails to identify all of the MAC requirements. Readers of this example may take this and use it as gospel. It is imperative that even the example reflects adequate design and development.

Recommendation. The policy for write-up should also be included.

4.12.3 (B.6) Various policies considered important in the TCSEC are missing from these examples including FPT_REV, FPT_RVM, FPT_SEP, FPT_TSA, etc.

Recommendation. The various policies should be added for closure.

4.13 - Annex C, Worked Examples - Firewall PP and ST

No Comment

4.14 - Annex D, Worked Examples - Database PP

No Comment

ATTACHMENT 5
to SC 27 N 2248rev1

German NB Comment on Project 1.27.22 (WD 15446) "Guide for production of Protection Profiles and Security Targets" (ISO/IEC JTC 1 SC 27 N 2172)

The German NB thanks the editor for providing a new WD 15446 (SC27 N2172). Due to the late delivery of the document only preliminary comments can be provided at the moment.

General comments:

A big problem regarding Protection Profile writing is the completeness problem. When is a PP complete, with regard both to security objectives and to functional components? One possible answer is to employ a best-effort method and revise the document if problems come up. Another method is to implement PP walk-throughs in analogy to code inspection reviews for design verification. A third method is independent expert review. The guidancedocument should propose these and other methods.

On the composability issue there is the following question: Is there a standard or recommended way of composing PPs, with regard to cross-citation of functional components and security objectives? If there are experiences they should be incorporated, otherwise this should be noted.

Detailed comments:

Section 5.2.1:

Figure 4 (?) does not have an identification.

Annex B:

Do the different font and bolding approaches have a technical meaning? Please explain or unify.

Annex F, Section 3.1:

The approach with giving special names to certain SFRs is somewhat ambiguous. On the one hand it is made clear how these SFRs have been derived from existing elements by using operations, on the other hand the use of specific names suggests, that the requirements have been explicitly stated. The fact that four elements are identified with DIGITSIG suggests, that these four elements could form a new component. It should be considered whether the example in Annex F should be used to explain how explicitly stated requirements can be used in a PP in a meaningful manner.